(1)

PERS-TR-91-002

PERSEREC

CONTINUING ASSESSMENT OF CLEARED PERSONNEL IN THE MILITARY SERVICES: REPORT 2 - METHODOLOGY, ANALYSIS, AND RESULTS

Michael J. Bosshardt
David A. DuBois

Personnel Decisions Research Institutes, Inc.

Kent S. Crawford

Defense Personnel Security Research
and Education Center

Dennis McGuire

Personnel Decisions Research Institutes, Inc.

January 1991

Approved for Public Distribution: Distribution Unlimited

DEFENSE
PERSONNEL SECURITY
RESEARCH AND EDUCATION CENTER
99 Pacific Street, Building 455-E
Monterey, California 93940-2481

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for public release,
distribution unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)
PERS-TR-91-002

6a. NAME OF PERFORMING ORGANIZATION
Personnel Decisions Research
Institutes, Inc.

6b. OFFICE SYMBOL *(If applicable)*

7a. NAME OF MONITORING ORGANIZATION
Defense Personnel Security Research
and Education Center (PERSEREC)

6c. ADDRESS *(City, State, and ZIP Code)*
43 Main Street SE, Riverplace, Suite 405
Minneapolis, MN 55414

7b. ADDRESS *(City, State, and ZIP Code)*
99 Pacific Street, Building 455E
Monterey, CA 93940-2481

8a. NAME OF FUNDING/SPONSORING ORGANIZATION
PERSEREC

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
N00014-87-D-0717 Del. Order 0005

8c. ADDRESS *(City, State, and ZIP Code)*
99 Pacific Street, Building 455E
Monterey, CA 93940-2481

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
Continuing Assessment of Cleared Personnel in the Military Services: Report 2--Methodology, Analysis, and Results

12. PERSONAL AUTHOR(S)
Bosshardt, Michael J., DuBois, David A., Crawford, Kent S. and McGuire, Dennis

13a. TYPE OF REPORT
Technical Report

13b. TIME COVERED
FROM Jan 89 TO May 90

14. DATE OF REPORT *(Year, Month, Day)*
1991 January

15. PAGE COUNT

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Continuing assessment, continuing evaluation, clearances, security, personnel security, security education

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

This is Report 2 in a series of four reports examining the effectiveness of continuing assessment programs in the military services. It discusses the analyses and results of a large-scale survey of security personnel and unit commanders at over 60 Army, Navy, Air Force, and Marine Corps sites worldwide. It describes how input from these groups was combined to identify key problem and recommendation areas, and serves as the foundation for Report 3 in this series.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION

22a. NAME OF RESPONSIBLE INDIVIDUAL
Roger P. Denk, Director

22b. TELEPHONE *(Include Area Code)*

22c. OFFICE SYMBOL

83 APR edition may be used until exhausted
All other editions are obsolete

PERS-TR-91-002 January 1991

CONTINUING ASSESSMENT OF CLEARED PERSONNEL IN THE MILITARY SERVICES: REPORT 2 - METHODOLOGY, ANALYSIS, AND RESULTS

Prepared by

Michael J. Bosshardt
David A. DuBois
Personnel Decisions Research Institutes, Inc.

Kent S. Crawford
Defense Personnel Security Research
and Education Center

Dennis McGuire
Personnel Decisions Research Institutes, Inc.

Defense Personnel Security Research and Education Center
Monterey, California 93940-2481

FOREWORD

The continuing assessment of cleared personnel is at the heart of an effective personnel security program. The intelligence and security community asked PERSEREC to conduct research in this key area since there was a basic lack of empirical information concerning the current effectiveness of continuing assessment programs. In order to address this requirement, we contracted with Personnel Decisions Research Institutes (PDRI), Inc. to assist us in conducting a major study to review continuing assessment programs operating in the field. We had three objectives: (1) to gather baseline information necessary for developing future research projects in continuing assessment, (2) to identify problem areas that were impacting on the effectiveness of continuing assessment, and (3) to provide specific recommendations for improving continuing assessment both in terms of new approaches and suggested policy changes.

The project resulted in four reports that provide a complete review and assessment of continuing assessment in terms of the above objectives. Each of the reports has the opening title of *Continuing Assessment of Cleared Personnel in the Military Services*. The reports are then differentiated as follows:

> Report 1 - *A Conceptual Analysis and Literature Review*. This report meets Objective 1 by providing a conceptual foundation for future research in continuing assessment and presenting a number of recommendations for specific research projects. The intended audience is primarily the research community.
>
> Report 2 - *Methodology, Analysis, and Results*. This report meets Objective 2 through discussing the analyses and results from a large-scale survey of over 60 military sites worldwide. It describes how input from security managers, unit security managers, and unit commanders was combined to identify key problem and recommendation areas. It serves as the foundation for Report 3. The intended audience for this report is security personnel who are interested in detailed and specific data concerning the operation of continuing assessment programs in the different services.
>
> Report 3 - *Recommendations*. This report addresses Objective 3 by outlining the principal findings and recommendations from the data collection effort described in Report 2. The specific objectives are to recommend policy changes and suggest approaches for improving the effectiveness of continuing assessment in military units. The intended audience is policymakers and security professionals.

Report 4 - *System Issues and Program Effectiveness*. This report also meets Objective 3 by taking a broader perspective and examining continuing assessment as a total system. This includes continuing assessment as it relates to other aspects of personnel security as well as different aspects of continuing assessment (e.g., periodic reinvestigations, position vulnerability, legal issues, automation issues, etc.). The focus here shifts from primarily a field perspective to consideration of continuing assessment as one part of a total security system. Again, the intended audience is policymakers and security professionals, although the issues tend to be discussed with regard to longer-term initiatives as opposed to the more short-term focus of Report 3.

Numerous persons assisted in this research project. The authors would like to express appreciation to the individuals who served as points of contact at each of the survey sites. These individuals arranged the site visits and served as gracious hosts and fine coordinators. The excellent survey participation rates and high quality of the data obtained attest to their conscientiousness and hard work. Additional thanks go to the many installation security managers, unit commanders, and unit security representatives who completed survey forms for the project.

At the service headquarters, appreciation goes to Walt Mestre, Jim Baxter, Coy Williamson, and George Jackson who greatly assisted the authors in identifying and scheduling visits to the field units. Daniel McGarvey, at the American Institutes for Research, provided valuable assistance during the data collection phase. At PDRI, mention should be made of the efforts of Dr. Walter Borman, who assisted in the survey data collection efforts. Dr. Borman also served as a general adviser throughout the project. Special thanks also go to two PDRI staff members for their contributions in carrying out this research: Deb Skophammer for her skillful editing and typing of this report and Kathy Lillie for her assistance in the data analyses. Finally, at PERSEREC, James Riedel provided extremely helpful input during both the design and implementation phases of the project.

We believe that these four reports, taken as a whole, provide a solid foundation for both improving current DoD policy with regard to continuing assessment and for developing new products and approaches for improving continuing assessment.

Roger P. Denk
Director

EXECUTIVE SUMMARY

Continuing assessment of cleared personnel is a critical component of Department of Defense (DoD) personnel security programs. There is limited information available, however, to determine the effectiveness of these continuing assessment efforts. In order to address this deficiency, a project was initiated to evaluate how well the continuing assessment program is operating in the military services. The primary focus was on continuing assessment programs for individuals with collateral clearances (i.e., Top Secret, Secret, and Confidential). The principal project activities included a review of regulations and literature related to continuing assessment and a survey of 60 Army, Air Force, Navy, and Marines Corps installations around the world to obtain detailed information about their continuing assessment programs.

This report is one of four project reports. It discusses the analyses and results of a large-scale survey of continuing assessment programs in the military services. The primary objectives of this report are to (1) provide baseline information for describing existing continuing assessment programs in the military services, (2) identify the major problems and obstacles encountered in these programs, and (3) suggest recommendations for improving continuing assessment programs.

The initial step in the project involved a series of meetings with headquarters and adjudication officials from the Army, Navy, and Air Force to gain an initial understanding of continuing assessment programs. Nine military installations were then visited to obtain an understanding of operational service branch continuing assessment programs and to gather information necessary for developing the research approach to be used during the survey phase.

Three survey forms were developed. The principal form was an interview protocol for installation security office representatives. Two shorter survey forms were also developed for unit security managers and unit commanders. These forms were based on several inputs: results of the site visits, findings of the literature review, results of discussions with headquarters continuing assessment policymakers and with adjudication facility personnel, reviews by continuing assessment experts, and a pilot test.

These survey forms were administered between September, 1989 and January, 1990. The survey sample included 60 sites (21 Air Force, 19 Army, 18 Navy, and 2 Marine Corps). Forty-eight sites were where individuals primarily had collateral access and 12 were sites where individuals primarily had SCI access; ten were overseas sites. Overall, survey data were received from 60 installation security office representatives, 126 unit security representatives, and 88 unit commanders.

The survey yielded five types of data: (1) ratings of 136 problems by security managers, unit security managers, and unit commanders; (2) listings of the major problems encountered by security managers, unit security managers, and unit commanders; (3) ratings of 143 recommendation items by security managers; (4) listings of recommendations for improving continuing assessment from security managers, unit security managers, and unit commanders; and (5) structured interview data from security managers. "Problems" were defined as obstacles in maintaining a highly effective continuing assessment program; "recommendations" were defined as ideas for improving continuing assessment.

In order to have a common basis for comparing the quantitative and qualitative data and to facilitate the interpretation of the survey results, a taxonomy of continuing assessment problem/recommendation, or "finding," areas was developed. This taxonomy included eight general categories: (1) security education/briefings/awareness; (2) training for security personnel: (3) derogatory information indicators/sources/methods; (4) adjudication facility/process; (5) accountability for continuing assessment; (6) continuing assessment regulations; (7) emphasis on continuing assessment; and (8) continuing assessment system considerations.

Analysis of continuing assessment survey data indicated that security education was the highest ranked of the eight continuing assessment taxonomy areas across all problem and recommendation data sets. Training for security personnel, continuing assessment system considerations, derogatory indicators/sources/methods, and the adjudication process received moderate to high rankings across the problem and recommendation data sets. Continuing assessment regulations and accountability for continuing assessment received the lowest overall rankings across data sets. Discussion of the specific areas within each category that received most emphasis is provided in this report.

Comparisons of the survey responses were also made according to several respondent characteristics: (1) primary level of access (SCI vs. collateral), (2) service branch (Army vs. Air Force vs. Navy), (3) geographic location (U.S. vs. overseas), (4) personnel type (civilian vs. military), (5) respondent type (security manager vs. unit security manager vs. unit commander), and (6) respondent tenure (longer term vs. shorter term). Results of these analyses indicated high levels of agreement between various groups (i.e., they perceived similar problems and made similar recommendations with regard to continuing assessment). However, some differences in continuing assessment program emphases, procedures, problems, and recommendations did emerge. These are discussed in the report.

Comparisons of survey responses from collateral and SCI sites suggested a high level agreement between data provided by respondents from both types of sites. The principal problem or finding areas which distinguished SCI and collateral continuing assessment programs were security education (collateral security staff consistently cited greater difficulties in this area), training for security staff (collateral respondents rated the quality of training for both installation and unit security staff higher than did SCI personnel), sources for gathering derogatory information (SCI security representatives rated unit personnel as the most useful sources of security-relevant information, whereas collateral site respondents gave top ratings to indirect sources such as the central adjudication facility, the police blotter, and the investigations office), issues concerning central adjudication (SCI personnel indicated greater difficulties with the clearance suspension and revocation process), and accountability for continuing assessment (collateral personnel cited a greater need for more inspection time on continuing assessment and suggested that incentives for performing continuing assessment duties have greater potential for contributing to program effectiveness).

TABLE OF CONTENTS

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

TABLES

TABLES (cont.)

APPENDICES

SECTION 1: INTRODUCTION

Problem

Keeping the nation's defense secrets is a problem of serious importance and immense scope. Each year millions of classified documents are produced and distributed to more than four million cleared individuals (General Accounting Office, 1986). Monitoring and assessing the reliability of cleared individuals to prevent the compromise of sensitive information is a primary objective of the personnel security program.

Recent history points to a need for improving personnel security practices. Espionage cases increased substantially during the 1980s, with more than 60 cases being identified by the authors. A number of additional cases may also have been investigated, although they remain unreported for a variety of reasons (e.g., to protect sensitive intelligence operations and sources, or to avoid exposure of classified information).

The damage incurred by the compromise of classified information can be enormous. A recent report by the United States Senate (1986) described the damage from espionage in several ways--it "seriously compromised" U.S. military plans and capabilities, "gravely impaired" U.S. intelligence operations, and overcame U.S. technological advantages in some areas (p. 12). The report estimated the financial impact of espionage during the 1980s to be in the billions of dollars. The wartime impact of these activities would be "devastating" (United States Senate, 1986, p. 104).

Within the Department of Defense, a personnel security program (Department of Defense, 1987; Director of Central Intelligence, 1986) is one of the principal approaches utilized to meet the threat of information compromise. This program has two major emphases. The first involves screening individuals who are being considered for initial clearances. The second emphasis, and the focus of this report, is the ongoing or continuing assessment of cleared personnel.

The importance of continuing assessment is underscored by several factors. For example, examination of recent espionage cases indicates that few spies enter government service with the intent to commit espionage. Instead, most individuals become spies as a result of personal and environmental circumstances that occur after job entry and after the granting of an initial security clearance. This suggests that an effective continuing assessment program is a critical element to deterring espionage.

Two other factors point to the importance of the continuing assessment program. First, initial clearance screening efforts are costly, involve conditions of very low base rates, and have unknown validity (Crawford, 1988; Fedor, 1988). Second, hostile intelligence activities probably focus more effort on currently cleared personnel than on uncleared individuals.

Although formal personnel security programs have been in existence for many years, concern has been expressed about the quality of these programs (U.S. House of Representatives, 1988). The Stilwell Report (DoD Security Review Commission, 1985) concluded the overall personnel security system is "reasonably effective" (p. 7), although they cited numerous recommendations for improving the system. A top-to-bottom security inspection of the military services found several deficiencies with operational personnel security programs (Secretary of the Army, 1986; Secretary of the Navy, 1987). Overall, however, little is known about the effectiveness of these operational continuing assessment programs.

The existing literature is small and consists almost entirely of narrative program descriptions, management analyses, and informed opinion (DuBois, Bosshardt, & Crawford, 1991). Only one research study on operational continuing assessment programs (Abbott, 1987) was located. This study examined continuing assessment programs in selected government agencies. Major problems with continuing assessment identified by Abbott included inadequate methods for assessing security-related behavior, the large number of personnel security clearances issued, and delays in conducting periodic reinvestigations. Abbott concluded that most continuing assessment programs should be improved and made several recommendations for achieving this objective. These recommendations included developing improved assessment procedures, developing improved security education and training, and integrating personnel security clearance data.

Overview of Continuing Assessment Requirements

The primary guidance for operational continuing assessment programs consists of DoD and service branch continuing assessment instructions. DoD Regulation 5200.2-R describes the basic requirements for the continuing assessment of personnel with collateral clearances. These requirements have been translated into service specific standards via AFR 205-32 for the Air Force, AR 380-5 and AR 380-67 for the Army, and 5510.1H for the Navy and Marine Corps. Each of these regulations/instructions outlines the requirements for continuing assessment programs at both the service and installation/command levels, including such areas as reporting requirements, reporting forms, security education requirements, and inspection program standards. Excerpts from each regulation/instruction for each requirement area are presented in Table 1.[1]

Although all services are guided by DoD requirements, important differences exist among them in the implementation of continuing assessment programs. Both the Navy and Army require that all adverse personnel information of security significance be forwarded to their central adjudication facilities, independent of whether the information is serious enough to warrant immediate suspension of access. The rationale for this policy is that a pattern of minor incidents across time may be significant enough to warrant a clearance revocation. The concern is that if central adjudication does not maintain this information, it could be lost or ignored as an individual is transferred from one assignment to another.

The Air Force, on the other hand, only requires the forwarding of adverse information when it is significant enough to warrant suspension of access. It is still possible, of course, for the individual's access to be reinstated if the information is later favorably adjudicated. In this program, minor incidents of personnel security significance are maintained in personnel records and dealt with by unit commanders and local installation and unit security managers.

An important structural difference also exists among the services with respect to their continuing assessment programs. The Army and Air Force tend to have a number of "units" operating within the context of an installation. Each unit has its own commander in addition to a unit security manager. Adverse information is usually forwarded from these units to a central security office at the installation. The installation security office subsequently forwards the information to the central adjudication facility. The installation security office can also uncover adverse information and coordinate with the unit commander responsible for the individual to determine whether the information should be forwarded to the central adjudication facility. Thus, with the exception of geographically remote units in the Army that deal directly with central adjudication, there are usually two separate but coordinated groups (unit and installation) that are involved in finding and processing adverse information. It should be noted, however, that personnel security information available to the unit commander and unit security manager may not be available to the installation security office.

[1] The Air Force (Regulation 205-32) provides the most detailed procedures for continuing assessment when compared with the other services; the Navy provides the least specific guidance.

Table 1

Excerpts from DoD and Military Collateral Regulations/Instructions Regarding Continuing Assessment Program Requirements

Component Item	DoD Collateral	Army Collateral	Navy Collateral	Air Force Collateral
Program Requirement	...the heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should ensure close coordination between security authorities and personnel, medical, legal, and supervisory personnel...(paragraph 9-100).	...Army commanders are responsible for the maintenance of an effective security posture within their activities. Each Army commander and agency head will...continually assess the individual trustworthiness of personnel who possess a security clearance. A commander may delegate authority to perform local security functions, but not the responsibility to do so (AR 380-5, paragraphs 13-304a.1 (e), 13-304a.2)...Personnel security functions are normally delegated to the installation DSEC/security manager/G-2, who will...report any adverse information (AR 380-5, paragraph 11-101h(5))...This program should ensure close coordination between security authorities and personnel, medical, legal, and supervisory personnel...(AR 380-67, paragraph 9-100).	Each command must have a program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties. Under this program, commands must establish internal channels for reporting information reflecting on an individual's loyalty, reliability and trustworthiness from a security perspective (paragraph 22-8 (1,2)). For effective management of the (information and personnel) program, the security coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties (paragraph 2-8 (3r)).	The Secretary of the Air Force maintains a program to evaluate the security eligibility status of personnel under his or her jurisdiction on a continuing basis. The purpose of this program is to ensure close coordination between security authorities, military and civilian personnel officials, medical, legal, and supervisory personnel so that all information available within a command is considered in the personnel security process (paragraph 7-1).
Reporting Requirement	Whenever derogatory information relating to the criteria and policy set forth in paragraph 2-200 and appendix I of this regulation is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security manager of the organization to which the individual is assigned (paragraph 8-101a.).	When the commanders learns of credible derogatory information on a member of his or her command that falls within the scope of paragraph 2-200, the commander will immediately forward DA form 5248-R to the Commander, CCF (paragraph 8-101b(1).	Commanding officers shall ensure continuous evaluation of assigned personnel for eligibility for access to classified information...Notify the DON CAF of any significant findings which may raise questions about an individual's eligibility, whether or not he/she holds a security clearance (paragraph 3-e (7)).	Whenever derogatory information relating to the criteria in paragraph 1-7 of this regulation is developed or otherwise becomes available to the Air Force or any other DoD element, it shall be referred by the most expeditious means to the base security police and commander of the organization to which the individual is assigned. The unit commander will review the information in terms of its security significance and completeness (paragraph 8-7).
Reporting Form	No specific form required. Left to discretion of the individual Service.	DA form 5248-R: Report of Unfavorable Information for Security Determination.	OPNAV 5510/41 - Personnel Security Action Request (paragraph 12, enclosure (1).	Special Security File (SSF).
Security Education Requirement	Commanders and heads of organizations shall ensure that personnel assigned to sensitive duties...are initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and on their individual responsibilities (paragraph 9-101).	Commanders and heads of organizations shall ensure that personnel assigned to sensitive duties are...initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and on their individual responsibilities (AR 380-67, paragraph 9-101)...The security education program shall...advise personnel of the requirements to report such matters as...information that could reflect adversely on the trustworthiness of an individual who has access to classified information (AR-380-5, paragraph 10-101j.3).	All command elements, particularly personnel, security, legal, medical, and supervisory personnel must understand that information which could place an individual's loyalty, reliability and trustworthiness in question has to be evaluated from a security perspective (paragraph 22-8(2))...The (command security education) program should be designed to: b. Advise personnel of their responsibility to adhere to the national standards of conduct required of persons holding positions of trust and to avoid behavior which could render them ineligible for access to classified information or assignment to sensitive duties; c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties; d. Advise supervisors of the requirement of continuous evaluation of personnel for eligibility for access to classified information or assigned to sensitive duties (paragraph 3-4 (3b, c, d).	Commanders (MAJCOM to unit level) must ensure that personnel assigned to sensitive duties...are initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and on their individual responsibilities (paragraph 7-2a)....Accordingly, the Secretary of the Air Force has established procedures to periodically brief persons requiring access to classified information...DoD 5200.1-R/AFR 205-1, chapter 10, outlines those procedures to meet the requirement of this section.
Inspection Requirement	The heads of DoD Components shall ensure that personnel security program matters are included in their administrative inspection programs (paragraph 11-103).	The heads of DoD Components shall ensure that personnel security program matters are included in their administrative inspection programs (paragraph 11-103).	Senior commanders are responsible for evaluating the effectiveness of the Information and Personnel Security Program in their subordinate commands. Inspections will be conducted by qualified personnel and will examine security management and procedures for...personnel security and security education (paragraph 2-18(1,2)).	MAJCOMs, SOAs, and selected DRUs conduct annual program reviews of their subordinate activities (paragraph 11-5b.). Program Administration. Review and evaluate: ...procedures used in the administration of SSFs (paragraph 11-6c(3)).

The Navy, on the other hand, has units/commands that interact directly with central adjudication. Each command has a commanding officer and a security manager. After coordination with the security manager, adverse information is forwarded directly from the commanding officer to the central adjudication facility. In large Navy commands (e.g., Naval Sea Systems Command), individual departments may have security coordinators who assist the security manager with the implementation of the security program. These coordinators may also pıovide the security manager with adverse information for personnel within their departments. However, it is the commander or commanding officer and his or her staff, who are the key decision-makers in the continuing evaluation process.

Continuing assessment programs also exist for individuals with access to sensitive compartmented information (SCI). General policy guidelines are provided by Director of Central Intelligence Directive No. 1/14. The Army program (which uses the 5248-R) is similar for individuals with either SCI or collateral access. In contrast, the Navy SCI community uses much more detailed procedures than its within-service collateral counterpart (including the use of a specially developed reporting form called the Special Access Evaluation Report or SAER). Finally, the Air Force SCI community has its own independent continuing assessment program. This program uses a Personal Data Report (PDR) to forward adverse information. Unlike the Air Force collateral program, Air Force SCI units are required to report all significant adverse information to their central adjudication facility (independent of whether the information resulted in a local immediate suspension of access).

This report examines how continuing assessment procedures are implemented across the services. One component of the DoD continuing assessment program which is not addressed in this report is the periodic reinvestigation (PR). Individuals with Top Secret or SCI access, or those who perform sensitive duties, are required to be reinvestigated every 5 years. This involves a follow-up background investigation conducted by the Defense Investigative Service. In addition, DoD makes limited use of the polygraph for personnel with very sensitive SCI access. While these additional tools are important, their limitations are that: (1) they are not generally used for personnel with Secret access; (2) they are not used frequently (e.g., only every 5 years for the PR); and (3) they do not make systematic ongoing use of critical personnel security information available at the unit/command and installation levels. Thus, although the periodic reinvestigation serves an important function, continuing assessment as performed at the local level must serve as the critical component of continuing assessment efforts.

Since this report discusses the results obtained from the Army, Air Force, and Navy, generic rather than service-specific terms are used. At the command, base, or installation level, personnel working on continuing assessment are referred to as "security managers." In the Army, security managers would refer to the personnel working within the installation security directorate (headed by the direcıor of security). In the Air Force, security managers refer to personnel working in the information security branch of the security police squadron. In the Navy, security managers refer to personnel in the command security office. At SCI sites, the corresponding position would be the Special Security Officer (SSO).

The phrase "unit security managers" is used in this report to refer to individuals working in operational and support units (as opposed to installation security managers who work in the installation or command security office). This phrase is also used differently among the various services. In the Army, it refers to the unit security manager and security staff (at the battalion level) and the activities security manager/staff (in support activities). In the Air Force, it refers to the individual (and occasionally, supporting staff) in the squadron who has the collateral duty of unit security manager. In large Navy commands, the unit security manager corresponds to the job of security coordinator. In smaller Navy commands, there is no position comparable to unit security manager.

Objectives

This report (Report 2) is one of four project reports. It describes the analyses and results from the survey of continuing assessment programs as implemented in the field. Report 1 (DuBois, Bosshardt, & Crawford, 1991) examines regulations and literature related to continuing assessment. Report 3 (Bosshardt, DuBois, & Crawford, 1991a) describes continuing assessment problems and recommendations as provided by field respondents. Report 4 (Bosshardt, DuBois, & Crawford, 1991b) examines several system issues related to continuing assessment, assesses the overall strengths and weaknesses of continuing assessment programs in the military services, and makes several recommendations for improving continuing assessment.

The primary objectives of this report are: (1) to provide baseline information describing existing continuing assessment programs in the military services, (2) to identify the major problems and obstacles encountered in these programs, and (3) to suggest recommendations for improving continuing assessment. To accomplish these objectives, a large-scale survey of continuing assessment programs at military installations throughout the world was undertaken. Survey information was gathered from three types of respondents (security managers, unit security managers, and unit commanders). Descriptions of the survey procedures and results are summarized in the following sections.

Organization of This Report

This report is organized into seven sections. Section 1 is this introduction. Section 2 describes the development of three continuing assessment survey forms and the procedures used to gather survey data from 60 military installations throughout the world. Section 3 describes the survey sample and the development of a taxonomy of continuing assessment finding areas.

Sections 4 and 5 describe the analyses of survey data obtained from collateral sites. Section 6 compares the survey responses of several different groups of respondents. Section 7 summarizes the major findings of this report.

SECTION 2: DEVELOPMENT AND ADMINISTRATION OF THE SURVEY INSTRUMENTS

This section describes the development and administration of three continuing assessment survey forms. These forms were developed on the basis of meetings with headquarters, adjudication, and field personnel and were subsequently administered to security personnel and unit commanders at 60 military installations throughout the world. Details of the survey form development and administration procedures are presented below according to the following topics: headquarters site visits, initial field site visits, adjudication facility site visits, DoD briefing, development of survey forms, pilot test of survey forms, survey sampling plan, and survey data collection procedures.

Headquarters Site Visits

The initial step in the project involved a series of 2- to 3-hour meetings with headquarters representatives from the Army, Navy, and Air Force in the Washington D.C. area. The dates and participants of each meeting are shown in Appendix 1 of the supplemental appendices[2]. During these meetings, information was obtained about the objectives and operation of service branch continuing assessment programs, gathered recommendations for improving continuing assessment, and determined the procedures necessary for visiting a sample of military installations.

These discussions with headquarters officials yielded approximately 40 distinct recommendations for improving continuing assessment. These recommendations included suggestions in the following areas: developing new procedures for gathering derogatory information on cleared personnel, obtaining additional derogatory information from installation or other sources, improving security education, increasing commander and supervisor accountability for continuing assessment, including continuing assessment as a performance appraisal or special interest IG item, examining the Personnel Reliability Program (PRP) for possible ideas, and developing personnel security regulation/manual supplements. A complete list of the recommendations is presented in Appendix A.

---

[2] This report has two sets of appendices. One set is attached with this report. A second set of appendices, called supplemental appendices, is provided in a separate document. These supplemental appendices provide additional documentation relevant to both this report and to Report 3 of this series.

Initial Field Site Visits

Nine military installations (two Army, two Air Force, and five Navy) in California were visited to: (1) obtain an initial understanding of the objectives and operation of service branch continuing assessment programs, (2) gather information necessary for developing the research approach to be used during the survey phase (e.g., determining whom to meet with, how long to meet with them, what questions to ask, what types of data to gather, the best methods for ¿ thering this data), and (3) obtain recommendations for improving continuing assessment. Appendix 2 of the supplemental appendices provides a complete listing of the sites, dates, and points of contact. Each site visit was conducted by one or two PDRI staff members, along with the PERSEREC contract monitor. Each visit lasted one day and included meetings with installation security staff members and with representatives from various installation departments (e.g., medical, personnel, military police).

Four structured interview protocols were used to obtain information from representatives of the security, medical, military police, and personnel departments during these initial site visits. Topics on all or most protocols included the general scope of continuing assessment program, personnel security areas and indicators, sources of continuing assessment information, reporting mechanisms and records, security education and awareness procedures, employee assistance programs, the effectiveness of continuing assessment programs, and recommendations for improving continuing assessment.

Site visit results indicated that three types of respondents should be sampled during the survey phase of the project: installation *security office representatives, unit security* representatives, and unit commanders. The results also suggested that meetings with installation department representatives (e.g., personnel, medical, military police, legal, employee assistance) would not be necessary during the larger follow-up survey because little unique information had been obtained in discussions with these officials.

The site visits provided considerable information about the operation and problems faced in military continuing assessment programs, as well as numerous recommendations for improving continuing assessment procedures. Overall, 40 unique suggestions for improvement were made in the following areas: obtaining additional derogatory information, improving and increasing security education and awareness, creating a security manager career field, providing more resources to the security office, improving clearance adjudication procedures, improving recordkeeping and reporting procedures, modifying personnel security regulations, instituting penalties for noncompliance with security regulations, reducing the amount of classified information, and reducing the number of cleared individuals. The complete list of suggestions is presented in Appendix 3 of the supplemental appendices.

Aojudication Facility Site Visits

Two 3-hour meetings were conducted with senior representatives of the Army Central Clearance Facility, the Air Force Security Clearance Office, and the Navy Central Adjudication Facility to discuss continuing assessment issues. Appendix 4 of the supplemental appendices lists the meeting dates and persons interviewed. The purposes of these meetings were to obtain a better understanding of the clearance (re)determination process and to obtain the input of senior adjudication personnel on issues related to continuing assessment.

DoD Briefing

Meetings were held with representatives of the Office of the Undersecretary of Defense (Security Policy) in July, 1989, to review project progress, the survey instrument, and the preliminary survey sampling plan. A number of modifications were made to the survey instrument and to the survey sampling plan as a result of this meeting.

Development of Survey Forms

Three survey forms were developed. The principal form was an interview protocol for installation security office representatives. Two shorter survey forms were developed for unit security managers and unit commanders. The development of each survey form is described below.

Security manager interview protocol. The interview protocol used during the initial field site visits served as a preliminary draft of the security manager survey protocol. This draft protocol was then revised according to: (1) results of the site visits, (2) findings of the literature review, (3) results of discussions with headquarters continuing assessment policy makers, and (4) results of discussions with adjudication facility personnel.

The revised security manager protocol was subsequently reviewed by several participants from the initial headquarters and field visits. These reviewers examined the instructions, items, and rating scales of the protocol for clarity and completeness. In response to reviewer comments, several items were modified or eliminated.

Unit security manager and unit commander survey forms. The unit security manager and unit commander survey forms were oriented toward the practical difficulties encountered in operating a continuing assessment program. Due to the limited time available for meeting with representatives from these groups (one hour), structured ratings were obtained concerning their perceptions of various problems associated with continuing assessment. To enable direct comparisons with the security manager results, the problem items on the security manager form were also used on the unit security representative and unit commander forms. However, to ensure that information about other continuing assessment problems could be obtained, an open-ended question about the three greatest problems in continuing assessment was added. In addition, respondents were asked to provide three recommendations for improving continuing assessment.

Pilot Test of Survey Forms

The three survey forms were pilot tested at Kirtland Air Force Base on 14 September 1989. Meetings were held separately with the installation security manager and with two senior Air Force continuing assessment policymakers to review the wording and completeness of the site visit interview protocol instructions, questions, and rating scales. Information about the time required to complete the interview protocol was also gathered.

One-hour meetings were then conducted with two unit security representatives and with two unit commanders to pilot test the other survey forms. During these meetings, participants completed the survey forms and provided feedback regarding the wording and completeness of the survey instructions, items, and rating scales. Survey form completion time information was also obtained

Members of the research team subsequently reviewed all suggested changes to the three survey forms and made several minor modifications to each form. Appendix 5 of the supplemental appendices presents the final version of each survey form.

Survey Sampling Plan

Our goal was to obtain continuing assessment information from a representative sample of Air Force, Army, and Navy sites, plus a small number of Marine Corps sites. The initial sampling plan was to randomly select 20 sites from each of the target service branches (i.e., Air Force, Army, Navy), plus two Marine Corps sites. However, several constraints precluded a truly random sampling procedure. Specifically, for each service branch we sought: (1) four sites with large proportions of personnel who had SCI access, (2) five OCONUS sites (two European, two Asian, and one Pacific) (3) four sites with a large proportion of civilian personnel, (4) sites in different geographic regions of the U.S., anu (5) several types of operational commands (e.g., tactical/strategic, intelligence, scientific/research and development, training, logistics/support, headquarters). In addition, for each target site, a backup site was sought with similar characteristics (i.e., same service branch, same command, same geographic region) in the event the visit to the primary site was canceled.

These many constraints precluded a truly representative survey sample. A breakdown of the final target number of sites according to service branch, level of access (collateral vs. SCI), and geographic location is presented in Table 2.

Table 2

Target Continuing Assessment Survey Site Sampling Plan:
Service Branch, Primary Access Level, and Geographic Location

	Service Branch				
Access Level- Geographic Location	Air Force	Army	Navy	Marine Corps	Totals
Collateral-U.S.	12	12	12	2	38
SCI-U.S.	4	4	5		13
Collateral-Overseas	4	4	3		11
TOTALS	20	20	20	2	62

Survey Data Collection Procedures

The site visit data were gathered between September, 1989 and February, 1990. The general data collection procedure included several steps. Prior to each site visit, a point of contact for the site was provided. A research team member then contacted this person to explain the purpose of the site visit and to arrange for the visit. A package was then sent to the point of contact which provided additional information about the project, confirmed the scheduled date, and included two sections of the site visit interview protocol (pp. 1 to 3; 25 to 42). Prior to the site visit, points of contact were to complete both sections of the protocol.

Each site visit was conducted by one research team member and lasted five to eight hours. Most of this time (four to five hours) was spent discussing the questions on pages 4 to 24 of the site visit interview protocol with one or more installation security managers These security manager(s) completed the rest of the protocol (pp. 1 to 3; 25 to 42) independently (usually prior to the site visit). A few security managers completed these sections after the site visit and mailed them back to the researcher.

Whenever possible, the researcher also conducted separate 1-hour meetings with a small number of (2 to 4) unit commanders and with a small number of (2 to 4) unit security managers/personnel.[3] During these group meetings, the researcher had participants independently complete the survey form. A discussion of continuing assessment issues generally followed completion of the surveys.

A brief report summarizing various impressions of the installation's continuing assessment program was written upon the completion of each site visit. In these reports, impressions of the best, worst, and most unique features of the program, suggestions for improving continuing assessment, and the conditions of the data collection were detailed.

[3] Several of the installations and commands visited had no units. At these sites, we met only with installation security representatives.

SECTION 3: DESCRIPTION OF SURVEY SAMPLE AND DEVELOPMENT OF A CONTINUING ASSESSMENT FINDING TAXONOMY

This section describes the final survey samples and the development of a taxonomy of topic areas for organizing the survey results. Each topic is discussed separately below.

Description of Final Survey Samples

Descriptive information was gathered regarding several characteristics of the survey sample, including site characteristics, respondent characteristics, clearance information, and the numbers and functions of personnel security staff members. Summaries of these descriptive variables are provided below.

Site characteristics. Survey data were collected from 60 sites, or 97 percent of the target number of sites. The complete list of participating sites is shown in Appendix B. Table 3 provides a breakdown of sites according to service branch (Army vs. Air Force, vs. Navy), primary access level of personnel (collateral vs. SCI), and geographic location (U.S. vs. overseas). Overall, the sample includes 48 collateral and 12 SCI sites. The sample includes 21 Air Force, 19 Army, 18 Navy, and 2 Marine Corps sites. Fifty sites are in the U.S. and 10 sites are overseas. Finally, the sample included 18 predominantly civilian sites (11 Army, 3 Air Force, 4 Navy) and 42 predominantly military sites (8 Army, 18 Air Force, 14 Navy, 2 Marine Corps).

Respondent characteristics. Overall, survey data were received from 63 installation security office representatives, 125 unit security representatives, and 88 unit commanders. Breakdowns of the survey respondents according to the three primary service branch samples (Army vs. Air Force vs. Navy), primary clearance orientation (collateral vs. SCI), and geographic location (U.S. vs. overseas) are presented in Appendix 6 of the supplemental appendices.

Table 4 presents a breakdown of the survey samples according to position tenure, time in security field, time as unit commander, time at installation, number of cleared individuals in unit, and time spent performing continuing assessment activities.

Clearance information. Table 5 presents clearance information for the survey sites (i.e., types and numbers of clearances, numbers of clearance suspensions, numbers of clearance revocations). Overall, the number of clearance suspensions and revocations during the past 12 months (per 1000 cleared individuals with this type of clearance/access) is very small. In more

Table 3

Continuing Assessment Survey Sites According to
Service Branch, Primary Access Level, and Geographic Location

	Service Branch				
Access Level- Geographic Location	Air Force	Army	Navy	Marine Corps	Totals
Collateral-U.S.	12	13	11	2	38
SCI-U.S.	5	3	4	-	12
Collateral-Overseas	4	3	3	-	10
TOTALS	21	19	18	2	60

Table 4

Composition of Survey Samples According Position Tenure, Time in Security Field, Time as Unit Commander, Time at Installation, Number of Cleared Individuals in Unit, and Time Spent Performing Continuing Assessment Activities

Respondent Characteristic	Installation Security Managers	Unit Security Managers	Unit Commanders
Average Time in Position (in years)	3.8	3.7	2.8
Average Time in Security Field (in years)	8.7	7.1	---
Average Time as Unit Commander (in years)	---	---	2.5
Average Time at Installation (in years)	5.6	6.2	4.5
Average Number of Cleared Individuals in Unit	---	487.7	226.5
Average Percentage of Time Spent on Continuing Assessment Activities	26.6	24.0	14.1

Note. The sample sizes varied for each item. For installation security managers, the sample sizes ranged from 49 to 53; for unit security managers, the sample sizes ranged from 103 to 121; for unit commanders, the sample sizes ranged from 58 to 82.

Table 5

Approximate Types and Numbers of Clearances, Numbers of Clearance Suspensions, Numbers of Clearance Revocations for Survey Sites

	Total Number (per site)		Approximate Number Suspended Per 1000 During the Past 12 Months (per site)		Approximate Number Revoked Per 1000 During the Past 12 Months (per site)	
	Mean	Median	Mean	Median	Mean	Median
Confidential Clearances	295.2	0.0	0.8	0.0	0.3	0.0
Secret Clearances	2847.0	875.0	4.2	0.7	0.5	0.0
Top Secret Clearances	583.4	144.5	1.2	0.0	0.1	0.0
Top Secret Clearance with SCI Access	678.9	106.0	2.4	0.0	1.8	0.0

Note. The sample sizes for these analyses ranged from 48 to 54.

than half of the sites there were no clearance or access revocations for any type of clearance or access and no clearance suspensions for individuals with confidential, top secret, or SCI access (per 1000 persons). Approximately 73 percent of all clearance suspensions and 56 percent of all clearance revocations were the result of continuing assessment activities. These numbers are based on estimates by installation security managers.

Numbers and functions of personnel security staff. Information was also obtained about the number of personnel security staff members and their allocation of time across different security functions. The average numbers of full- and part-time security office staff members were 5.1 and 1.7, respectively. According to estimates by installation security managers, they spent an average of 26.6 percent of their time on continuing assessment duties, 37.6 percent on other personnel duties (excluding continuing assessment), 18.3 percent on other security duties (excluding personnel security), and 18.1 percent of their time on non-security duties. Corresponding percentages for unit security managers were 16.4, 16.1, 16.5, and 49.4 percent. The average number of personnel security positions authorized at these sites visited was 3.2. The average number of personnel security positions filled was 2.8.

Development of a Problem/Recommendation Taxonomy

The continuing assessment survey yielded a considerable amount of quantitative and qualitative information regarding both the problems encountered in continuing assessment and suggestions for improving continuing assessment procedures. In order to have a common basis for comparing the quantitative and qualitative data and to facilitate the interpretation of the survey results, a taxonomy of continuing assessment problem/recommendation or "finding" areas was developed.

The development of a taxonomy of continuing assessment findings involved a series of steps. The first step was to examine available survey information concerning the problems encountered in continuing assessment and various suggestions for improving continuing assessment programs. This process included reviewing 136 rated problem items, 143 rated recommendation items, 684 write-in problems with continuing assessment provided by survey respondents, and 636 write-in suggestions for improving continuing assessment provided by survey respondents. Next, these items were sorted into eight general categories: (1) security education/briefings/awareness, (2) training for security personnel, (3) derogatory information indicators/sources/methods, (4) adjudication facility/process, (5) accountability for continuing assessment, (6) continuing assessment regulations, (7) emphasis on continuing assessment, and (8) continuing assessment system considerations. The items within each of these categories were then sorted by the authors into two to six subcategories of related items. These subcategories provide additional information about the content of each major category area.

The final taxonomy of continuing assessment categories and subcategories is presented in Table 6. A listing of the specific problem and recommendation items classified into each category and subcategory is provided in Appendix 7 of the supplemental appendices.

The means for each item were subsequently computed across all collateral respondents. For each category and subcategory, the average of the means for individual items in that category or subcategory was also computed. This was done separately for both the problems and recommendations items. Results of these analyses will be presented in Section 4.

In addition to rating these problem and recommendation items, respondents described what they considered to be the top three problems with respect to the continuing assessment program and the top three recommendations for improving it. Results of both sets of analyses are also presented in Section 4.

Table 6

Continuing Assessment Taxonomy Categories and Subcategories

1. Security Education/Briefings/Awareness
   1a. Security education for unit commanders, supervisors
   1b. Security education for cleared personnel
   1c. Security education/awareness materials
   1d. Security awareness

2. Training for Security Personnel
   2a. Training for security office staff
   2b. Training for unit security managers

3. Derogatory Information Indicators/Sources/Methods
   3a. Security risk indicators
   3b. Reporting/information from cleared individuals
   3c. Reporting from/cooperation with unit personnel
   3d. Reporting from/cooperation with installation groups
   3e. Reporting from/cooperation with non-installation sources
   3f. Recordkeeping procedures

4. Adjudication Facility/Process
   4a. Timeliness and effectiveness of clearance adjudication
   4b. Interaction with/access to adjudication facility

5. Accountability for Continuing Assessment
   5a. Accountability for continuing assessment responsibilities
   5b. Incentives/consequences for security-relevant behavior
   5c. Continuing assessment in performance appraisals
   5d. Inspections with respect to continuing assessment
   5e. Program effectiveness indicators

6. Continuing Assessment Regulations
   6a. Security regulations

7. Emphasis on Continuing Assessment
   7a. Top management/DoD commitment to continuing assessment
   7b. Resources/funding devoted to continuing assessment
   7c. Personnel security staffing
   7d. Career field for security personnel

8. Continuing Assessment System Considerations
   8a. Targeting continuing assessment to particular groups
   8b. Continuing assessment system deficiencies
   8c. Legal issues related to continuing assessment
   8d. Number of cleared personnel/classified documents
   8e. Periodic reinvestigation procedures
   8f. Clearance pre-screening procedures

SECTION 4: ANALYSES OF CONTINUING ASSESSMENT SURVEY RATING DATA FOR COLLATERAL SITES

This section describes results of the continuing assessment survey of security managers, unit security managers, and unit commanders at collateral sites. Discussion of the results according to several contextual factors (e.g., level of access, service branch, geographic location, respondent type) is presented in the next section. Additional discussion of the principal survey findings in terms of problems and recommendations is presented in Report Three of this series.

The discussion for this section is organized according to four general topic areas: (1) reliability of the problem and recommendation ratings, (2) analyses of the problems or obstacles encountered in continuing assessment, (3) analyses of the recommendations for improving continuing assessment, and (4) summary of the problems/recommendations analyses. Our discussion focuses on the major survey findings and includes a number of summary tables. Numerous additional tables and more detailed statistical information can be found in supplemental Appendix 8.[4]

Reliability of the Problem and Recommendation Ratings

Estimates of the statistical reliability of the problems and recommendations ratings were computed to determine the extent to which various groups of respondents agreed upon their problem and recommendation judgments. For each group of persons using the survey form, we should expect relatively high agreement between their responses to the problem and recommendation items.

Respondents in the overall sample and within each of eight groups (i.e., security managers, unit security managers, unit commanders, collateral site respondents, SCI site respondents, Army respondents, Navy respondents, Air Force respondents) were first randomly divided into two subgroups. Mean profiles across the 136 problem items and across the 143 recommendation items were computed for each of these 16 subgroups. For each subgroup pair (e.g., two subgroups of security managers), correlations were computed between the two mean subgroup item profiles. The Spearman-Brown formula was then used to estimate the reliability of the judgments based on the full sample for each group. For the problem ratings, the reliability estimate for the overall sample was .96; reliability estimates for the eight specific respondent groups ranged from .80 to .95. For the recommendations ratings, the reliability estimate for the overall sample was .89; reliability estimates for six respondent groups (unit security managers and unit commanders did not make these ratings) ranged from .55 to .81.

----

[4] Because of the very small number of sites sampled (N=2), results for the Marine Corps are not discussed.

Overall, the results indicate respondents within each particular group showed relatively high agreement with respect to their perceptions of the problems encountered in continuing assessment and moderate agreement regarding their recommendations for improving continuing assessment. However, it should be noted that the reliability estimates did vary somewhat across the different groups, primarily because of the differences in sample sizes for these groups.

Analysis of Continuing Assessment Problems

Survey respondents (security managers, unit security managers, and unit commanders) provided two types of information regarding the problems or obstacles faced in continuing assessment. First, respondents rated each of 136 items according to "how much of an obstacle it is in maintaining a highly effective continuing assessment program" using a scale from "0" (not a problem) to "10" (major problem). (A listing of all problem items and the rating scale instructions is given in section 3 of the security officer interview protocol in Appendix 5 of the supplemental appendices.) In addition, respondents wrote down the three biggest problems they encountered in maintaining and managing an effective continuing assessment program. Results of both sets of analyses are described separately below.

Problem item ratings. Table 7 presents mean problem ratings for each of the 8 major categories and 30 subcategories in the continuing assessment taxonomy for all collateral respondents. (The reader will recall these means represent the average of the means of the individual items included in each category or subcategory[5].) Examination of the results for the eight major categories indicates that training for security personnel, security education/briefings/awareness and the adjudication facility/process are the three most highly rated categories (based on the mean of the item ratings in each category). Less highly rated categories include continuing assessment system considerations, accountability for continuing assessment, derogatory information indicators/sources/methods, emphasis on continuing assessment, and continuing assessment regulations.

Mean ratings for the 30 subcategory areas (based on the mean of the problem item ratings in each subcategory) are also shown in Table 7. The results indicate that concerns over the timeliness and effectiveness of clearance adjudication is the most highly rated subcategory. Three concerns about security education (security education for cleared personnel, security education for commanders and supervisors, and security education/awareness materials) are

[5] Mean ratings for all 136 problem items for the entire sample and for several subgroups (collateral site respondents, SCI site respondents, security managers, unit security managers, and unit commanders) are presented in Appendix C.

Table 7

Continuing Assessment Categories and Subcategories Rank Ordered According to Mean Ratings on the Problem Items[1] (Sample = 224 Collateral Site Respondents)

Problem Category	Mean Rating
2. Training for Security Personnel	5.0
1. Security Education/Briefings/Awareness	4.8
4. Adjudication Agency/Process	4.6
8. Continuing Assessment System Considerations	4.1
5. Accountability for Continuing Assessment	4.0
3. Derogatory Information Indicators/Sources/Methods	3.9
7. Emphasis on Continuing Assessment	3.9
6. Continuing Assessment Regulations	3.1

Problem Subcategory	Mean Rating
4a[2]. Timeliness and effectiveness of clearance adjudication.	5.8
1b. Security education for cleared personnel.	5.2
2b. Training for unit security managers.	5.1
1a. Security education for unit commanders, supervisors.	5.0
1c. Security education/awareness materials.	5.0
2a. Training for security office staff.	4.9
8c. Legal issues related to continuing assessment.	4.9
5e. Program effectiveness indicators.	4.8
3b. Reporting/information from cleared individuals.	4.6
5b. Incentives/consequences for security-relevant behavior.	4.5
7c. Personnel security staffing.	4.5
8d. Number of cleared personnel/classified documents.	4.5
3a. Security risk indicators.	4.3
7d. Career field for security personnel.	4.3
3c. Reporting from/cooperation with unit personnel.	4.2
8a. Target continuing assessment to particular groups.	4.1
8e. Periodic reinvestigation procedures.	4.0
1d. Security awareness.	3.9
5c. Continuing assessment in performance appraisals.	3.9
3e. Reporting from/cooperation with non-installation sources.	3.8
3d. Reporting from/cooperation with installation groups.	3.7
8f. Clearance pre-screening procedures.	3.7
5a. Accountability for continuing assessment responsibilities.	3.6
7b. Resources/funding devoted to continuing assessment.	3.5
8b. Continuing assessment system deficiencies.	3.5
4b. Interaction with/access to adjudication facility.	3.4
5d. Inspections with respect to continuing assessment.	3.4
7a. Top management/DoD commitment to continuing assessment.	3.2
6a. Security regulations.	3.1
3f. Recordkeeping procedures.	3.0

[1] Item ratings were made on a "0" (not a problem) to "10" (major problem) scale.

[2] The number in the subcategory designation (e.g., the "4" in 4a) refers to the general category to which this subcategory belongs (e.g., 4. Adjudication Agency/Process). See Table 6 for more information.

among the five most highly rated subcategories. Concerns about training for security personnel (for both unit and base security managers) also received high mean ratings.

Table 8 presents the 26 problem items with the highest ratings, organized according to the 8 categories of the continuing assessment taxonomy. (The reader should note that this table is based on actual item means and not means of groups of items such as the category or subcategory means.) Although the number of items for each category should be interpreted with caution because some categories had many more items than other categories, the content of these items does provide information about the specific a eas of continuing assessment considered most problematic by field personnel. Common themes in Table 8 include inadequate security education activities and materials, reluctance to report derogatory information, problems with the clearance adjudication process, insufficient staff time for continuing assessment, and difficulties in obtaining continuing assessment information. The six most highly rated problem items, ranked ordered by mean item rating, are: (1) the reluctance of individuals to self-report derogatory information; (2) the time taken by central adjudication facility to make clearance decisions; (3) the reluctance of coworkers to report derogatory information; (4) a lack of training modules to instruct commanders and supervisors on how to spot, interpret, and manage the early warning indicators of personnel security risk; (5) inadequate continuing assessment training for supervisors; and (6) a lack of standard training modules for commanders, supervisors, and cleared individuals which describe their continuing assessment responsibilities.

Problem write-in responses. In addition to rating 136 problem items, survey respondents described what they considered to be the three greatest problems encountered in maintaining, managing, and assisting in the management of an effective continuing assessment program. These open-ended responses were grouped according to the category framework presented earlier. Table 9 presents a summary of the number of times each type of problem was mentioned for the 8 categories and 30 subcategories of the continuing assessment taxonomy. The results indicate that derogatory information indicators/sources/methods, emphasis on continuing assessment, and continuing assessment system considerations were the most commonly cited areas. Other categories mentioned (rank ordered according to the number of times the area was mentioned), include adjudication facility/process, security education/briefings/awareness, continuing assessment regulations, training for security personnel, and accountability for continuing assessment.

The results in Table 9 indicate that concerns about personnel security staffing and system deficiencies (e.g., lack of consolidation of continuing assessment program elements across service branches) were the most frequently mentioned subcategories. Other subcategories mentioned at least 30 times include security education for unit commanders and supervisors, reporting from and cooperation with unit personnel, security regulations, timeliness and effectiveness of adjudicative process, training for unit security managers, and top management/DoD commitment to continuing assessment.

Table 8

Problem Items With the Highest Mean Ratings
Organized by Continuing Assessment Category
(Sample = 224 Collateral Site Respondents)

1. Security education/briefings/awareness:

- Lack of/inadequate training modules to instruct commanders and supervisors on how to on how to spot, interpret, and manage the early warning indicators of personnel security risks.
- Lack of standard training modules for unit commanders, supervisors, and cleared individuals which describe their continuing assessment responsibilities.
- Inadequate continuing assessment training for supervisors.
- Lack of training aids (e.g., handouts, desk references) to assist supervisors in identifying individuals who have security-related problems.
- Lack of videotapes to train personnel in their continuing assessment responsibilities.
- Inadequate continuing assessment training for unit commanders.
- Inadequate continuing assessment training for cleared individuals.
- Derogatory information sources are not familiar with their continuing assessment reporting responsibilities.
- Insufficient security education activities in the area of continuing assessment.

2. Training for security personnel:

- Inadequate continuing assessment training for unit security managers.

3. Derogatory information indicators/sources/methods:

- Reluctance of individuals to self-report derogatory information.
- Reluctance of coworkers to report derogatory information.
- Difficulties obtaining derogatory information on cleared individuals.
- Difficulties obtaining derogatory information on cleared individuals when they are off the installation.
- Reluctance of persons to report derogatory information because of concern about hurting the individual's career.
- Lack of formal reporting procedures and written standards for personnel, medical, legal, and other departments defining what information should be shared with the security office.

Table 8 (cont.)

4. Adjudication facility/process:

   - Too much time is taken by central adjudication facility to make clearance suspension/revocation decisions.
   - Delays in obtaining replacement personnel for individuals who lose security clearances.
   - Security office has insufficient access to central adjudication facility.

5. Accountability for continuing assessment:

   - Lack of knowledge regarding which aspects of the continuing assessment program are most effective.

6. Continuing assessment regulations:

   [No items]

7. Emphasis on continuing assessment:

   - Insufficient time for unit security managers to perform their continuing assessment responsibilities.
   - Understaffing of the personnel security office.
   - Lack of a separate, full-time position for personnel security managers.

8. Continuing assessment system considerations:

   - Difficulties obtaining derogatory information on civilians.
   - Existing laws and privacy act restrictions make it difficult to obtain continuing assessment-relevant information on cleared individuals, especially civilians.
   - Difficulties monitoring large numbers of cleared persons.

Table 9

Continuing Assessment Categories and Subcategories Rank Ordered According to Number of Times Each Type of Problem Was Mentioned (Sample = 224 Collateral Site Respondents)

	Problem Category	Frequency
3.	Derogatory Information Indicators/Sources/Methods	143
7.	Emphasis on Continuing Assessment	122
8.	Continuing Assessment System Considerations	107
4.	Adjudication Agency/Process	65
1.	Security Education/Briefings/Awareness	62
6.	Continuing Assessment Regulations	42
2.	Training for Security Personnel	39
5.	Accountability for Continuing Assessment	23

	Problem Subcategory	Frequency
7c.	Personnel security staffing.	67
8b.	System deficiencies.	63
1a.	Security education for unit commanders and supervisors.	48
3c.	Reporting from/cooperation with unit personnel.	43
6a	Security regulations.	42
4a.	Timeliness and effectiveness of adjudicative process.	38
2b.	Training for unit security managers.	36
7a.	Top management/DoD commitment to continuing assessment.	31
3d.	Reporting from/cooperation with installation groups.	28
4b.	Interaction with/access to adjudication facility.	27
3f.	Recordkeeping procedures.	25
3b.	Reporting/information from cleared individuals.	24
8d.	Number of cleared personnel/classified documents.	22
3a.	Security risk indicators.	14
7d.	Career field for security personnel.	14
1c.	Security education/awareness materials.	11
5a.	Accountability for continuing assessment responsibilities	10
7b.	Resources/funding for continuing assessment.	10
8e.	Periodic reinvestigation procedures.	10
3e.	Reporting from/cooperation with non-installation sources	9
8a.	Target continuing assessment to particular groups.	8
5b.	Incentives/consequences for security-relevant behavior.	5
5e.	Program effectiveness indicators.	5
1d.	Security awareness.	3
2a.	Training for security office staff.	3
5d.	Inspections with respect to continuing assessment.	3
8c.	Legal issues related to continuing assessment.	2
8f.	Clearance pre-screening procedures.	2
1b.	Security education for cleared personnel.	0
5c.	Continuing assessment in performance appraisals.	0

Comparisons of the results for the rated problem items and open-ended responses show some consistent patterns. The adjudication facility/process and continuing assessment system consideration problem areas each received moderate emphasis from both the rated items and the open-ended responses. Accountability for continuing assessment and continuing assessment regulation areas each received relatively low emphasis in both sets of data. However, the two top-rated categories (training of security personnel, security education) each had only a moderate number of write-in responses. Similarly, the two most frequently mentioned write-in problem areas (derogatory information indicators/sources/methods and emphasis on continuing assessment) each received relatively low ratings.

Analysis of Continuing Assessment Recommendations

Security managers provided two types of information regarding recommendations for improving continuing assessment. First, respondents rated 143 items according to their "potential contribution for improving continuing assessment" using a scale from "0" (would not improve continuing assessment) to "10" (major contribution for improving continuing assessment). (A listing of all recommendation items and the rating scale instructions is presented in the security officer interview protocol in Appendix 5.) In addition, security managers wrote down their top three recommendations for improving continuing assessment. Results of both sets of analyses are presented separately below.

Recommendation item ratings. Table 10 provides a breakdown of the mean ratings (based on the average of the means of the individual items included in each category or subcategory) for each of the categories and subcategories of the continuing assessment taxonomy.[6] In general, the results are similar to the problem ratings and indicate that training of security personnel and security education/briefings/awareness are rated as the most important categories for improving continuing assessment procedures.

Mean ratings for each of the 30 subcategory areas (based on the average of the means of the individual items included in each subcategory) are also shown in Table 10. The results indicate that security education has the two most highly rated subcategories and three of the five top rated subcategories. Improving training for unit security managers is the third most highly rated subcategory; reducing system deficiencies is the fourth most highly rated subcategory.

[6] The mean ratings for all 143 recommendation items for the entire sample, for collateral personnel, and for SCI personnel are presented in Appendix D.

Table 10

Continuing Assessment Categories and Subcategories Rank Ordered According to Mean Ratings on the Recommendations Items[1] (Sample = 44 Collateral Site Security Officers)

Recommendation Category	Mean Rating
2. Training for Security Personnel	6.6
1. Security Education/Briefings/Awareness	6.4
8. Continuing Assessment System Considerations	5.9
6. Continuing Assessment Regulations	5.8
5. Accountability for Continuing Assessment	5.5
4. Adjudication Agency/Process	5.4
3. Derogatory Information Indicators/Sources/Methods	5.3
7. Emphasis on Continuing Assessment	5.2

Recommendation Subcategory	Mean Rating
1b.[2] Improve security education for cleared personnel.	7.2
1a. Improve security education for unit commanders and supervisors.	7.1
2b. Improve training for unit security managers.	7.1
8b. Reduce system deficiencies.	6.7
1c. Improve security education/awareness materials.	6.7
5b. Provide incentives/consequences for security-relevant behavior.	6.4
8d. Reduce the number of cleared personnel/classified documents.	6.4
2a. Improve training for security office staff.	6.2
8f. Improve clearance pre-screening procedures.	6.1
8a. Target continuing assessment to particular groups.	6.1
5e. Develop program effectiveness indicators.	6.1
7d. Develop a career field for security personnel.	6.0
4b. Improve interaction with/access to adjudication facility.	5.9
6a. Improve security regulations.	5.8
3c. Improve reporting from/cooperation with unit personnel.	5.8
3d. Improve reporting from/cooperation with installation groups.	5.7
8c. Resolve legal issues related to continuing assessment.	5.6
3a. Improve security risk indicators.	5.5
5d. Improve inspections with respect to continuing assessment.	5.4
7c. Increase personnel security staffing.	5.4
7a. Increase top management/DoD support for continuing assessment.	5.3
3e. Improve reporting from/cooperation with non-installation sources.	5.2
5c. Include continuing assessment in performance appraisals.	5.0
4a. Improve timeliness and effectiveness of adjudicative process.	5.0
3f. Improve recordkeeping procedures.	4.9
5a. Improve accountability for continuing assessment responsibilities.	4.8
3b. Improve reporting/information from cleared individuals.	4.7
1d. Improve security awareness.	4.4
8e. Improve periodic reinvestigation procedures.	4.4
7b. Increase resources/funding for continuing assessment.	4.3

[1] Item ratings were made on a "0" (not a problem) to "10" (major problem) scale.

[2] The number in the subcategory designation (e.g., the "1" in 1b) refers to the general category to which this subcategory belongs (e.g., 1. Security Education/Briefing Awareness). See Table 6 for more information.

Table 11 presents the 28 recommendation items with the highest ratings, organized by category area.[7] Common themes in Table 11 include improving security education for various groups, improving security education training materials, improving continuing assessment training for security managers and for unit security managers, improving the clearance adjudication process, instituting penalties to increase accountability for continuing assessment, and increasing staffing for continuing assessment. The five items with the highest ratings are to: (1) create a separate, full-time position for personnel security managers; (2) improve continuing assessment training for supervisors; (3) develop training modules to instruct commanders and supervisors on how to spot and manage the early warning indicators of personnel security risks and personnel problems; (4) modify the regulations to direct other installation groups to provide more derogatory information to the security office; and (5) ensure that derogatory information sources are familiar with their continuing assessment responsibilities.

Recommendation write-in responses. At the conclusion of the recommendation item ratings, survey respondents wrote down their top three recommendations for improving continuing assessment. These open-ended responses were grouped according to the category framework presented earlier. Table 12 presents a summary of the number of times each recommendation area was mentioned for each category and subcategory. The results indicate that emphasis on continuing assessment and continuing assessment system and security education/briefings/awareness are the commonly suggested areas for improvement. Derogatory information indicators/sources/methods and continuing assessment system considerations are other categories with a relatively high number of suggestions.

The most frequently mentioned subcategories in the write-in responses portion of the survey include improving security education for unit commanders and supervisors, developing a career field for security personnel, improving security regulations, increasing personnel security staffing, improving the timeliness and effectiveness of adjudicative process, and improving security education/awareness materials.

Comparisons of the results for both sets of recommendation data (rated items and open-ended responses) show some consistent trends. Security education was the second most highly ranked area in both sets of recommendations; continuing assessment system considerations and adjudication facility/process received moderate emphasis from both sets of information; and accountability for continuing assessment and continuing assessment regulations received relatively low emphasis in both sets of data. However, the top-rated category (training for security staff) has only a moderate number of write-in responses. Similarly, the two most frequently mentioned write-in problem areas (derogatory information indicators/sources/methods and emphasis on continuing assessment) have relatively low ratings.

[7] Since the number of items varied for each category, the reader should not interpret the number of items listed as a true indicator of the overall importance of the category.

Table 11

Highly Rated Recommendation Items
Organized by Continuing Assessment Category
(Sample = 44 Collateral Site Security Officers)

1. Security education/briefings/awareness:

   - Ensure derogatory information sources are familiar with their continuing assessment responsibilities.
   - Increase security education activities related to continuing assessment.
   - Conduct more/better refresher briefings on continuing assessment responsibilities.
   - Conduct more/better initial briefings on continuing assessment responsibilities.
   - Improve continuing assessment training for supervisors.
   - Improve continuing assessment training for unit commanders.
   - Improve continuing assessment training for cleared individuals.
   - Develop training modules to instruct commanders and supervisors on how to spot and manage the early warning indicators of personnel security risks and personnel problems.
   - Develop training aids (e.g., handouts, desk references) to assist supervisors in identifying individuals who have security-related problems.
   - Develop standard training modules for unit commanders, supervisors, and cleared individuals which describe their continuing assessment-related responsibilities.
   - Increase the number of security education personnel.

2. Training for security personnel:

   - Increase/improve continuing assessment training for security managers.
   - Increase/improve continuing assessment training for unit security managers.

3. Derogatory information indicators/sources/methods:

   - Develop formal reporting procedures and written standards for the personnel, medial, legal, and other departments which define the types of information to be shared with the security office.

Table 11 (cont.)

4. Adjudication facility/process:

   - Reduce the time required by central adjudication facility for processing clearance suspensions/revocations.
   - Increase central adjudication facility phone lines/staff to provide more availability to the installation security offices.
   - Increase the number of hours that the security office has access to central adjudication facility.

5. Accountability for continuing assessment:

   - Institute/enforce penalties for falsifying continuing assessment forms.
   - Institute/enforce penalties for individuals who do not submit required periodic continuing assessment paperwork before the five year limit.
   - Develop better indicators for assessing the effectiveness of the continuing assessment program at each reporting level.

6. Continuing assessment regulations:

   - Modify the regulations to direct other installation groups (e.g., medical, personnel, legal, employee assistance) to provide more derogatory information to the security office.
   - Provide more guidance in the regulations on reporting requirements and implementation of continuing assessment procedures, especially to groups that make record reviews.

7. Emphasis on continuing assessment:

   - Take actions which encourage top levels/senior executives to make continuing assessment a higher priority.
   - Increase number of personnel security office staff.
   - Increase the number of security education personnel.
   - Create a separate, full-time position for personnel security managers.

8. Continuing assessment system considerations:

   - Take steps to improve the "attitude towards personnel security" among installation personnel.
   - Reduce the number of persons requiring access to classified information.

Table 12

Continuing Assessment Categories and Subcategories Rank Ordered According to Number of Times Each Type of Recommendation Was Mentioned (Sample = 44 Collateral Site Security Officers)

	Recommendation Category	Frequency
7.	Emphasis on Continuing Assessment	124
1.	Security Education/Briefings/Awareness	112
3.	Derogatory Information Indicators/Sources/Methods	86
8.	Continuing Assessment System Considerations	71
4.	Adjudication Facility/Process	52
2.	Training for Security Personnel	44
6.	Continuing Assessment Regulations	43
5.	Accountability for Continuing Assessment	35

	Recommendation Subcategory	Frequency
1a.[1]	Improve security education for unit commanders and supervisors.	47
7d.	Develop a career field for security personnel.	46
6a.	Improve security regulations.	43
7c.	Increase personnel security staffing.	40
4a.	Improve timeliness and effectiveness of adjudicative process.	34
1c.	Improve security education/awareness materials.	33
2b.	Improve training for unit security managers.	28
3f.	Improve recordkeeping procedures.	26
7a.	Increase top management/DoD support for in continuing assessment	26
8b.	Reduce system deficiencies.	19
4b.	Improve interaction with/access to adjudication facility.	18
1b.	Improve security education for cleared personnel.	17
5b.	Provide incentives/consequences for security-relevant behavior.	17
2a.	Improve training for security office staff.	16
8c.	Resolve legal issues related to continuing assessment.	16
1d.	Improve security awareness.	15
3c.	Improve reporting from/cooperation with unit personnel.	14
3a.	Improve security risk indicators.	13
8d.	Reduce the number of cleared personnel/classified documents.	13
3d.	Improve reporting from/cooperation with installation groups.	12
7b.	Increase resources/funding for continuing assessment.	12
8e.	Improve periodic reinvestigation procedures.	12
3b.	Improve reporting/information from cleared individuals.	11
3e.	Improve reporting from/cooperation with non-installation sources	10
5a.	Improve accountability for continuing assessment responsibilities	8
8f.	Improve clearance pre-screening procedures.	7
5d.	Improve inspections with respect to continuing assessment.	5
8a.	Target continuing assessment to particular groups.	4
5e.	Develop program effectiveness indicators.	3
5c.	Include continuing assessment in performance appraisals.	2

[1] The number in the subcategory designation (e.g., the "1" in 1a) refers to the general category to which this subcategory belongs (e.g., 1. Security Education/Briefings/Awareness). See Table 6 for more information.

Summary: Rated and Write-in Problems and Recommendations

In summary, the results indicate that security education was the most highly ranked of the eight continuing assessment taxonomy areas across problem and recommendation data sets. Training for security personnel, continuing assessment system considerations, derogatory information indicators/sources/methods, and the adjudication facility process received moderate to high rankings across the problem and recommendation data sets. Continuing assessment regulations and accountability for continuing assessment received the lowest overall rankings across data sets.

The results, however, were affected by the data collection method used. Category rankings of rated problems and rated recommendations are highly similar, as are category rankings based on the number of write-in problems and the number of write-in recommendations. However, the category rankings for rated and write-in problems are quite different, as are the category rankings for the rated and write-in recommendations.

SECTION 5. ANALYSES OF CONTINUING ASSESSMENT SURVEY INTERVIEW DATA FOR COLLATERAL SITES

This section describes the results of structured interviews with 48 installation security managers at collateral sites on various topics related to continuing assessment. (The specific interview questions are presented on pages 4 to 24 of the interview protocol presented in Appendix 5 of the supplemental appendices.) The discussion for this section is organized according to the eight continuing assessment taxonomy categories presented in Table 6. More detailed information regarding the interview results is presented in Appendix E of this report and in Appendix 8 of the supplemental appendices. Appendix E provides summaries of the responses to 58 open-ended interview questions organized by service branch. Appendix 8 of the supplemental appendices provides summaries of the quantitative interview information.

Security Education

Respondents were questioned about several topics related to security education. These included participation in security education, the specific content of security education, the general understanding of continuing assessment responsibilities, and recommendations for improving security education. Results for each area are presented below.

Participation in security education activities related to continuing assessment is moderately high. Approximately 69 percent of cleared personnel who required access to classified information on a daily basis and 53 percent of non-cleared personnel participated in security education in the past 12 months.

Specific questions regarding the content of security education indicate that approximately 76 percent of the programs provide information on the individual's continuing assessment responsibilities, about 79 percent provide guidance on reporting derogatory information, approximately 69 percent provide information on personnel security indicators, and about 43 percent provide guidance on obtaining employee assistance or counseling.

Regarding briefings related to continuing assessment, approximately 88 percent of the respondents indicated that initial briefings contain information on continuing assessment, with an average of 33 percent of these briefings devoted to continuing assessment. About 70 percent of the respondents noted that refresher briefings contain continuing assessment information, with an average of 35 percent of these briefings devoted to continuing assessment. Of the refresher briefings which cover continuing assessment topics, almost all (96 percent) included security threats, 81 percent discussed security risk indicators and 85 percent discussed reporting mechanisms.

The security managers interviewed believed that supervisors and cleared individuals understand their continuing assessment responsibilities only moderately well and that non-cleared individuals understand their responsibilities even less well. Using a 10-point rating scale (where "1" = does not understand continuing assessment responsibilities; "10" = understands continuing assessment responsibilities extremely well), the mean ratings were 5.2 for supervisors, 5.0 for cleared individuals, and only 3.2 for non-cleared individuals.

The most frequently mentioned ideas for improving security education and briefing procedures related to continuing assessment were improving security education training content and materials, increasing the amount of security education and time devoted to briefings, having more and better videos, increasing the resources (time, personnel, money) devoted to security education and briefings, and providing more guidance on security risk indicators. Other promising ideas to improve security staff training include having non-security personnel (e.g., supervisors, unit commanders, Defense Investigative Service (DIS) or agency representatives, persons who committed violations, department points of contact) provide security education training and briefings; developing standard security education courses; and including continuing assessment in supervisor, commander, and installation department training courses. The complete list of ideas is presented in Appendix E.

Training

Respondents rated the quality of security training for security office staff and for unit security managers as only moderate overall (approximately 4.6 on a 10 point score). When asked what could be done to improve the effectiveness of continuing assessment training for security staff, the most frequent suggestions were to increase the amount of training and to improve training materials. Other ideas to improve security staff training included increasing resources for training, developing a correspondence course for security staff, having mobile training teams, having interview skills training, having field trips to DIS and the adjudication facility, enforcing security regulations, making training more interesting, having intelligence personnel administer training, certifying training personnel, and making persons accountable for attending training.

When asked what specific topics are not adequately covered in security manager training, the most frequent responses included: security risk indicators, preparing continuing assessment forms, the adjudication process and adjudication standards, personnel security in general, administering a continuing assessment program, derogatory information reporting procedures, continuing assessment in general, security counseling procedures, and interviewing techniques. Other topics mentioned included handling security investigations, processing derogatory information, teaching security education, training security staff members, the initial screening process, sources of derogatory information, interacting with officials in other departments, clearance termination procedures, security awareness procedures, and legal aspects of continuing assessment.

Derogatory Information Indicators, Sources, and Methods

A significant portion of the interview protocol addressed the process of gathering security-related information. Specific topic areas covered included the types of derogatory information gathered, sources of valid derogatory information, recommendations for improving information reporting from various groups (e.g., subjects, unit commanders, supervisors, coworkers, unit security managers, installation departments, other installation security offices, other installations) and recordkeeping procedures. Each of these topic areas is discussed separately below.

Types of derogatory information. Security managers estimated the number of valid derogatory incidents reported to the security office during the past year for each of 12 types of information. The mean number of reported incidents for each area is shown below:[8]

- alcohol abuse (56.2)
- other incidents such as Nonjudicial punishments (NJPs), conflicts of interest, shoplifting (44.2)
- drug abuse (30.8)
- criminal felony acts not covered in other categories (15.7)
- court martials/desertions (14.6)
- financial problems (14.3)
- falsification of information acts (12.5)
- emotional/mental/family problems (11.7)
- security violation incidents (9.6)
- sexual misconduct (7.2)
- foreign associations/travel incidents (0.5)
- disloyalty to the U.S. (0.3)

Overall, respondents estimated that approximately 90 percent of reported derogatory information is valid.

The two types of derogatory information which account for most clearance revocations or discharges are alcohol and drug abuse incidents. Of the incidents that are known to other persons at the installation, the three types least likely to be reported are financial problems, emotional/mental/family problems, and alcohol abuse.

[8] It should be noted that these numbers varied considerably across sites, partially because the installations differed significantly in size. The average number of cleared persons at these sites was approximately 4622.

Sources of valid derogatory information. Table 13 presents ratings by security managers regarding the willingness of various groups to share information of security relevance with the security office. The results indicate that coworkers and supervisors are rated among the most unwilling to share information with the security office. Several installation departments (e.g., employee assistance groups, medical, personnel, legal) also received low to moderate ratings. Not surprisingly, coworkers and subjects received the lowest ratings.

Table 14 presents information regarding the number of sites in which various sources report derogatory information directly to the security office and the usefulness of these sources in providing the security office with information to be forwarded to the central adjudication facility. The sources that most frequently report security-relevant information to the security office are the central adjudication facility, investigations office, police blotter, supervisors, unit commanders, and the military police. In contrast, the sources least likely to report information directly to the security office are dropboxes, chaplains, non-law enforcement databases, informants, neighbors, hotlines, and postcards.

Overall, the most useful sources of security-relevant information (as rated by security managers), are the police blotter, the military police, the central adjudication facility, the investigations office, random drug testing, other installation/commands, and unit commanders. Sources rated least useful include subjects, other (non-police) local authorities, coworkers, and local newspapers.

When asked to identify which sources of continuing assessment information have the most unrealized potential usefulness, the most frequently mentioned were coworkers, supervisors, and medical/employee assistance groups. Less frequently mentioned sources included existing computer databases (e.g., NCIC), commanders, the personnel department, credit information, the legal department, local authorities, headquarters and other commands, investigations offices, the polygraph, informants, subjects, family members, and dropboxes.

Respondents were asked whether any additional sources of security-relevant information not listed in Table 14 are used, and what additional sources of information should be used. Approximately 10 percent of the respondents used additional sources of information such as credit information, periodic reinvestigations, personal/pre-indoctrination interview results, inspection results, and information from ex-spouses. The most frequently mentioned additional sources of information which should be used were credit/financial information, family members, friends, and ex-spouses. Other sources which respondents said should be used more frequently include local mental health/social agencies, national agency check information, central adjudication agency information, drug testing for civilians, previous housing offices, and polygraph results.

Table 13

Mean Ratings by Installation Security Managers of the Willingness of Various Groups to Share Continuing Assessment Information With the Security Office

Group	N	Mean Rating
Military Police	37	8.7
Other Base Security Office(s)	31	8.3
Central Adjudication Facility	41	8.1
Investigations Office	41	7.9
Installation Commanders	32	7.3
Unit Security Managers	34	7.3
Unit Commanders	37	7.1
First sergeant	37	6.8
Legal Department	41	6.5
Other Installations/Commands	41	6.3
Local Civilian Police	36	6.0
Federal Agencies	31	5.9
Supervisors	43	5.8
Medical Department	41	5.7
Personnel Department	40	5.5
Other Local Authorities	32	5.1
Employee Assistance Groups	38	3.9
Coworkers	41	3.2
Subjects	41	2.3

Note. The scale used ranged from "1" = Very unwilling to "10" = Very Willing.

Table 14

Number of Sites in Which Various Sources of Security Information Report Directly to the Security Office and Mean Ratings by Collateral Installation Security Managers of the Usefulness of These Sources

Source	N	Mean Rating
Dropboxes	1	10.0
Chaplains	1	10.0
Police Blotter	33	8.8
Military Police	32	8.7
Central Adjudication Facility	36	8.2
Investigations Office	35	8.1
Random Drug Testing	25	8.0
Other Base Security Office(s)	20	8.0
Other Computer Databases	1	8.0
Unit Commanders	32	7.8
Medical Department	20	7.7
Legal Department	19	7.7
First sergeant	23	7.5
Federal Agencies	13	7.5
Installation Commanders	14	7.4
Employee Assistance Groups	10	7.4
Unit Security Managers	26	7.3
Personnel Department	17	7.2
Supervisors	32	7.1
Local Civilian Police	21	7.0
Law Enforcement Databases	14	6.9
Other Installations/Commands	24	6.7
Subjects	16	6.6
Other Local Authorities	10	6.2
Coworkers	19	5.7
Local Newspapers	20	5.1
Informants	7	5.1
Neighbors	6	5.0
Hotline Information	6	3.8
Postcards	3	1.7

Note. The scale used ranged from "1" = Very little usefulness to "10" = Extremely useful.

Improving information reporting from various groups. Discussions with security managers indicated that unit commanders and supervisors are sometimes reluctant to report derogatory information. The three most commonly cited reasons for this reluctance were concerns about operational readiness/unit mission accomplishment, concerns about hurting the individual's career, and the perception that the problem reflects the commander's or supervisor's leadership. Other reasons mentioned included a lack of knowledge regarding what should be reported, the time commitment and paperwork required, the fear of reprisals or legal problems, and the belief that they (i.e., commanders, supervisors) can handle the problem.

A series of questions asked about changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office by each of the following groups: subjects, coworkers, supervisors, unit commanders, unit security managers, the personnel department, the medical department, the legal department, the military police, other security offices on the installations, other installations, and the investigations office. Brief summaries of the principal recommendations for each group are provided below. More detailed information is presented in Appendix E.

Subjects. Three primary suggestions were made to increase self-reporting by subjects. These were: (1) providing limited amnesty or reducing punishment for those who self-report derogatory information, (2) increasing the frequency and amount of security education/briefing information related to continuing assessment, and (3) having cleared individuals complete a self-report form or interview.

Unit commanders and supervisors. The principal recommendation for improving the reporting of personnel security information by unit commanders and supervisors was to improve and to increase security education and awareness. Other frequently mentioned suggestions included incorporating continuing assessment as a performance appraisal item for commanders and supervisors; enforcing reporting requirements and creating consequences for not reporting known derogatory information; providing anonymity and amnesty, if requested, to individuals who report derogatory information; developing standard forms for periodically evaluating the security worthiness of cleared subordinates on each of several derogatory information areas; and providing a stronger continuing assessment mandate in the regulations for unit commanders.

Coworkers. The two primary suggestions for improving reporting by coworkers of cleared individuals were to improve/increase security education and awareness in the area of continuing assessment and to provide anonymity and amnesty, if requested, to those who report derogatory information.

Unit security managers. The most frequent suggestions for improving reporting by unit security managers were to increase/improve security education and awareness for unit personnel, to increase/improve training for unit security managers, and to make security a primary duty or full-time job for unit security managers (especially for those in larger units). A fourth suggestion mentioned less frequently was to include continuing assessment as a performance appraisal item for unit security managers.

Installation departments. Respondents offered numerous ideas for improving the reporting of continuing assessment information by installation groups (e.g., personnel, medical, legal, employee assistance, military police, and the investigations office). Most frequently cited were: (1) to increase security education for department representatives and include continuing assessment reporting responsibilities as part of the training for department officials, (2) to incorporate continuing assessment reporting requirements into department regulations and provide more guidance regarding the types of information that should be shared with the security office, (3) to provide the security office with greater access to continuing assessment-relevant records and files kept by other department groups, and (4) to improve communication with department officials. Two additional ideas for improving reporting by installation departments were: (1) to have memoranda of agreement between the security office and various installation departments which specify what information will be shared between offices; and (2) to develop standard forms which departments can use to report derogatory information to the security office.

Other installation security offices. Surprisingly, some respondents noted that other security offices at their installation are sometimes reluctant to share security-relevant information. Recommendations for improving the sharing of information between installation security offices included improving and increasing communication, having common training and security education to emphasize the importance of sharing information, and establishing formal procedures for sharing information.

Other installations. Several security managers indicated that other installations are sometimes reluctant to share security information. Establishing better procedures for sharing derogatory information was the principal suggestion for improving cooperation between installations. Using standard derogatory information report forms, letters, or checklists which are completed by the command transferring the individual and which accompany his/her records is one means of accomplishing this. Other ways to better share derogatory information included improving the contact with other security offices via annual security manager meetings, improving the physical transfer of derogatory information to prevent cleared individuals from removing or altering copies of continuing assessment-relevant records during transfers (e.g., prohibit hand carrying of security-relevant records, telefax files, or send files via express or registered mail), and incorporating information sharing into the regulations. Two additional ideas emerging from these interviews were to develop a book containing a list of all security managers and their phone numbers, and to use automated channels to transfer information.

Other considerations in reporting. Approximately 90 percent of the respondents thought that some units do a much better job than others of reporting valid derogatory information to the security office. Several factors contributed to these differences in reporting performance. These factors include differences in the knowledge, experience, and training of unit personnel, as well as their interest and commitment. Additional contributing factors cited were the sensitivity of the unit's mission, the amount of classified information, the personnel resources devoted to unit security, the quality of the security education program, the relationship with installation security office, and the extent to which structured data gathering forms are used.

Not surprisingly, survey respondents suggested that unit commanders have access to more security-relevant information than does the security office. They estimated that, on average, about 47 percent more information would be obtained if derogatory information were forwarded simultaneously to both the security office and the unit commander.

Continuing assessment recordkeeping. A series of questions in the survey/interview protocol addressed continuing assessment recordkeeping procedures, including the types of security information maintained, the types of information not available to the security office, the types of information purged, the transfer of continuing assessment information between commands, and recommendations for improving recordkeeping procedures. Each of these topics is discussed briefly below.

Most of the collateral offices surveyed maintained separate files containing continuing assessment information on cleared individuals. The most common types of information contained in these files are security violations, security incidents, and local violations. Other types of information often included personal history information, disciplinary actions, NJPs, and personnel information. A few sites also kept security-related performance appraisal information in their files. In addition, approximately 48 percent of the security offices surveyed prepare periodic reports related to continuing assessment.

When asked what critical information relevant to continuing assessment the security office needs but does not have access to, the most commonly cited areas were medical, employee assistance, disciplinary, and criminal information. Other frequently mentioned areas included financial information, drug and alcohol information, and personnel records.

Some security-related information is purged when cleared individuals transfer or reenlist. When asked what types of purged information should be kept to better enable continuing assessment, the most commonly mentioned items were security and disciplinary violations (e.g., Article 15s, NJPs, letters of reprimand). Other types of information mentioned include employee assistance group records, police records and blotter information, letters of clearance suspension and revocations, and financial information.

Several respondents expressed concerns about the current procedures used for transferring continuing assessment information from one command to another. Common suggestions for improving this process included creating a standard security checklist or report form, preventing individuals from hand carrying security records, using telefax or express/registered mail to transfer records, including more derogatory information into the records, having more timely submissions, and using automated channels for transferring information. One interesting additional idea was administrating a self-report form at the time of transfer.

Several ideas were suggested for improving continuing assessment recordkeeping procedures. The most common idea was to automate personnel security records and retain these records in a central repository. Other ideas mentioned less frequently included developing standard recordkeeping procedures and forms, increasing staffing and equipment devoted to recordkeeping, developing new reports (such as a monthly unit security manager report), and reexamining existing guidelines concerning what should be purged from files during transfers or reenlistments.

Adjudication Facility/Process

Two questions requested information about how much derogatory information reaches unit commanders and the central adjudication facility in the adjudication process. Approximately 80 percent of the respondents indicated that significant derogatory information reaches unit commanders most, but not all, of the time. Fifty-five percent of respondents indicated that everything known or received by the security office is forwarded to the adjudication facility. Of course, not all information should be forwarded unless the security office and unit commander agree that it has personnel security significance.

A related issue concerns which type of continuing assessment program is better, one which reports only significant derogatory information to the adjudication facility and suspends an individual's access, or one which reports all derogatory information to adjudication and may or may not suspend an individual's access. Approximately 60 percent of the respondents indicated that reporting all information is preferable because of the need to assess the whole person and to have historical information. In contrast, those who recommended reporting only significant information argued that some information is not relevant, that adjudicators sometimes overreact to certain information, and that forwarding all information to adjudication would be inefficient. This issue will be discussed more thoroughly in Report 4 of this series.

Accountability for Continuing Assessment

Several interview questions examined issues relating to accountability foı carrying out continuing assessment responsibilities. Specific areas addressed regarding accountability issues included indicators of program effectiveness, commander accountability, performance appraisals, incentives, and inspections. Each topic is discussed separately below.

Indicators of continuing assessment program effectiveness. Three questions were asked about the types of indicators used by the security office and by installation commanders to assess the effectiveness of the continuing assessment program. Results for each question are summarized below.

Most of the installations surveyed maintain statistics relevant to continuing assessment. Most commonly, statistics are kept regarding the numbers and types of clearances, the numbers of clearance suspensions and revocations, and the numbers of derogatory incidents or report forms submitted to the security office. Other statistical indicators mentioned included the numbers of periodic reinvestigations, the numbers of security violations, statistics on inspection results and foreign travel records, the amount of classified information available to personnel, the number of security violation reports to the commander, and security education/briefing records.

Approximately 80 percent of the security offices used one or more indicators to evaluate the effectiveness of their continuing assessment program. Program effectiveness indicators most frequently mentioned involved the number of security violations, the number of reported derogatory incidents or incident reports, the number of derogatory information files created, and the number of clearance suspensions or revocations. Other indicators mentioned included: the results of inspections, office assistance visits, self-inspections, and program reviews; feedback from unit security managers or commanders; the timeliness of periodic reinvestigations; the results of training exercises; and the number participating in security education and training courses.

Approximately 67 percent of installation commanders used one or more indicators to monitor the effectiveness of the continuing assessment program. The most frequently used indicators included the number of security violations, the number of clearance suspensions or revocations, and the results of inspections, office visits, and program reviews. Other indicators mentioned included reports from or meetings with the security office, the absence of complaints about security, the numbers and types of clearances, training records, the results of training exercises, and the currency of security-related investigations.

Improving commander accountability in continuing assessment. Security office personnel provided several suggestions for improving the accountability of installation and unit commanders in continuing assessment. Frequently cited suggestions were to include continuing assessment as an inspection or performance appraisal item, to keep installation commanders better informed of continuing assessment procedures/policies, and to increase security education and career training activities related to continuing assessment for installation commanders. Another interesting idea was to have the installation commander certify annually that the continuing assessment program has been reviewed.

Frequent suggestions for increasing the involvement and support of unit commanders in the continuing assessment process were to increase security education and career training activities related to continuing assessment, to include continuing assessment as an inspection or performance appraisal item, to make the reporting of derogatory information a requirement, and to enforce regulations. Other interesting ideas involving the support of unit commanders included keeping them better informed of continuing assessment matters via meetings, updates, and status reports; creating penalties for noncompliance with security regulations; and requiring unit commanders to administer security education.

Performance appraisals. Only a small percentage of individuals are evaluated on security as part of their performance evaluation. According to estimates provided by installation security managers, 8 percent of unit commanders, 11 percent of supervisors, and 7 percent of cleared non-supervisory personnel are evaluated on security. Even fewer individuals are evaluated specifically on continuing assessment--about 2 percent of unit commanders and supervisors.

Incentives. Using incentives to improve the reporting of derogatory information is a controversial issue. Approximately 27 percent of the respondents indicated that incentives should not be used. Among those who supported the use of incentives, several possible types were mentioned. These included recognition, commendations, medals, letters of appreciation, plaques, certificates of accomplishment, monetary awards, notices in the paper, special liberty, and a letter in personnel file for persons who are exceptionally conscientious in performing their continuing assessment duties.

Inspections. Approximately 20 percent of personnel security inspection time is devoted to continuing assessment across participating sites. About 80 percent of the those interviewed indicated that inspectors use several types of indicators to evaluate the effectiveness of the continuing evaluation program. These include examining records for currency, accuracy, organization (e.g., comparing roster of cleared persons having derogatory information with personnel file, comparing headquarters files with command files, or ensuring appropriate reports are being made); numbers and types of special security files, derogatory report forms, security violations, or Article 15s; the number of persons who had their clearances suspended; and the timeliness of periodic reinvestigations. Several other indicators are listed in Appendix E.

The most common suggestion for improving the inspection process in the area of continuing assessment was to have standard inspection checklists and standards. Other interesting suggestions included having more inspections and increasing the thoroughness of inspections; devoting more resources (personnel, time) to inspections; improving training for inspectors; interviewing supervisors, unit commanders, and cleared individuals during inspections; providing better training for inspectors; increasing inspection statistics; having inspectors provide more feedback and training; spot checking records; and including continuing assessment as a special interest item on the IG.

Continuing Assessment Regulations

Security managers were asked to evaluate the adequacy of: (1) locally developed continuing assessment regulations, (2) service branch continuing assessment regulations, (3) the 5200.2-R, and (4) the DCID 1/14 on a scale from "1" (highly inadequate) to "10" (excellent) scale. Mean ratings for all regulations were moderately high and very similar, ranging from 6.3 to 7.0.

Security managers were asked what could be done to improve each of the regulations (as cited above). The most frequent suggestions for improving the local regulations were to provide more specific information and to keep this information up-to-date. For the service branch and DoD regulations, the most common recommendations were: to make them more detailed; to make them easier to understand by better indexing, organization, and cross-referencing of materials; to improve command/department support; and to clearly specify the responsibilities of installation departments. The principal suggestion for improving the DCID 1/14 was to make this regulation more specific.

Emphasis on Continuing Assessment

Security managers were asked to estimate the priority that each of 18 groups places on continuing assessment. Table 15 summarizes the results. These results indicate that senior intelligence personnel, other security offices, and the investigations office place the most emphasis on continuing assessment. Coworkers, non-supervisory personnel, and several installation groups (personnel, medical, employee assistance) place the least emphasis on continuing assessment.

Respondents additionally reported that personnel who do not have security clearances generally receive less continuing assessment emphasis than those with clearances. Specifically, 62 percent of the respondents reported giving either less emphasis, much less emphasis, or no emphasis to persons without clearances. However, 78 percent of the respondents suggested that persons without clearances should be included in the continuing assessment program, despite current funding levels. Reasons for this included: they (non-cleared individuals) might obtain access later, they have responsibilities to report information of security significance, they could be exposed to classified information, and they may possess important (nonclassified) information. In contrast, reasons cited for not including personnel without clearances in the continuing assessment program were lack of program resources, and the additional amount of time and paperwork involved by including these individuals in the program.

Approximately 53 percent of the respondents indicated that persons with clearance eligibility (i.e., having security clearances but no access to classified information) receive about the same continuing assessment emphasis as do cleared individuals with access to classified information.

Table 15

Mean Ratings by Collateral Installation
Security Managers of the Priority Placed
on Continuing Assessment by Different Groups

Group	N	Mean Rating
Senior Intelligence Personnel	31	7.4
Other Base Security Office(s)	30	7.3
Investigations Office	41	7.1
Military Police	37	7.1
Unit Security Managers	33	6.5
Installation Commanders	40	6.2
Unit Commanders	36	6.1
Firsc sergeant	36	5.9
Federal Agencies	36	5.9
Other Commands	37	5.5
Legal Department	41	5.0
Supervisors	42	4.9
Medical Department	41	3.9
Non-supervisory Personnel With Access to Classified Information	41	3.9
Personnel Department	42	3.7
Employee Assistance Groups	42	3.4
Non-supervisory Personnel Without Access to Classified Information	40	2.9
Coworkers	42	2.8

Note. The scale used ranged from "1" = Very low priority to "10" = Very high priority.

About 38 percent of the collateral installations surveyed target more continuing assessment effort toward persons with Top Secret access than to persons with Secret access. The most common additional activity for Top Secret personnel is the periodic reinvestigation. In some installations, Top Secret personnel may also receive better information, more briefings, or more training. When asked how much continuing assessment emphasis should be given to individuals with Secret vs. Top Secret access given current funding levels, 52 percent of the sample indicated that both groups should receive the same emphasis, 44 percent suggested Top Secret personnel should receive more emphasis, and 4 percent indicated both groups should receive more emphasis.

Approximately 45 percent of the security managers interviewed noted that more continuing assessment effort is directed to particular positions at their installations (excluding PRP billets). The types of positions which most often receive greater attention include those with Top Secret or SCI access as well as those in special access programs, presidential support programs, or SIOP programs. These additional continuing assessment procedures include more careful supervision of cleared personnel, more frequent and thorough briefings, more careful monitoring of personnel records, and random polygraphs.

About half of the sample suggested that there are special challenges associated with the continuing assessment program which are unique or which occur more frequently in certain geographic locations. Special difficulties cited for U.S. installations (compared to overseas sites) included having: less control over individuals, more privacy act protections for individuals, less emphasis on continuing assessment, increased drug usage, and fewer closely knit work groups. Special problems cited for overseas sites (compared to U.S. sites) include closer proximity to designated countries, increased travel by cleared individuals to designated countries, difficulties created by foreign laws, large naturalized populations at some bases, cultural differences, greater difficulty communicating with the central adjudication facility, more marriages to local nationals, and the high cost of living in some areas.

Almost 90 percent of the respondents suggested that more continuing assessment emphasis should be targeted to installations located in certain geographic areas. Areas most frequently mentioned included overseas areas, areas near or in designated countries/consulates, Europe (especially Germany), the Far East (especially Korea), the Baltic/Mediterranean countries, California (especially near San Francisco), Washington D.C./Norfolk, high threat areas, and high cost areas. One respondent noted that different aspects of the continuing assessment program should be emphasized depending on the specific risks of the location.

Continuing Assessment System Considerations

The eighth continuing assessment taxonomy category involves various system considerations related to the continuing assessment process and to the personnel security system as a whole. One critical issue concerning this system is the effectiveness of the continuing assessment program and its various components. As noted earlier, the survey results indicate that few existing measures of continuing assessment effectiveness are used. No procedures for systematically comparing the adequacy of different components within the continuing assessment program were found.

Effectiveness of continuing assessment components. In order to obtain preliminary information regarding the adequacy of different continuing assessment components, respondents were asked to rate the current and potential effectiveness of various continuing assessment components using a scale from "0" (component not used) to "10" (very effective). Table 16 summarizes the results.

With respect to current effectiveness, the results in Table 16 indicate that the component with the highest rating (clearance suspension/revocation process) received only a "moderately effective." Other highly ranked components included sources of derogatory information, service branch regulations, security risk indicators, reporting procedures, security education, security briefings, and DoD security regulations. In contrast, the two components rated the lowest were performance appraisal information and incentives for reporting.

Table 17 presents the ratings of the current and potential effectiveness of these continuing assessment program components by collateral security managers from the Army, Air Force, and Navy. The current effectiveness ratings for these different components are generally similar across service branches. However, there are some differences. Navy collateral security managers rated the following components much lower than other service representatives: unit security staff training in CA, indicators of CA program effectiveness, and inspections/staff assistance visits (related to CA). Army representatives rated the current effectiveness of the DoD security regulations much higher than did representatives from the other services.

The results in Table 17 also indicate the potential effectiveness ratings of these components are generally similar across service branches. However, some differences exist. Navy collateral security managers rated DoD security regulations and incentives for reporting derogatory information much lower than did representatives from the other services. Army representatives rated the current effectiveness of the DoD security regulations much higher than did the other services.

With respect to potential effectiveness, the most highly rated components were sources of derogatory information, the clearance suspension/revocation process, service branch regulations, security education, security office training, and continuing assessment reporting procedures. All of these components had ratings in the "potentially very effective" range. Examining the differences between current and potential effectiveness ratings, the components with the largest mean differences (indicating the greatest potential for improvement) are incentives for reporting, security office training in continuing assessment, performance appraisal information, inspections/staff visits related to continuing assessment, and employee assistance programs.

Table 16

Mean Ratings by Collateral Installation Security Managers of the Current and Potential Effectiveness of Various Continuing Assessment Program Components

Continuing Assessment (CA) Program Component	Mean Current Effectiveness	Mean Potential Effectiveness
Clearance Suspension/Revocation Process	6.7	8.5
Sources of Derogatory Information	5.8	8.8
Service Branch CA Regulations	5.6	8.4
Indicators of Security Risk	5.4	8.1
Overall Continuing Assessment for Military Personnel	5.2	8.4
CA Reporting Procedures	5.0	8.3
Security Education (related to CA)	5.0	8.4
Security Briefings (related to CA)	4.9	7.9
DoD Security Regulations	4.8	7.1
Local CA Regulations	4.7	7.7
CA Recordkeeping Procedures	4.6	7.8
Coordination of CA Information With Other Groups	4.0	7.9
Unit Security Staff Training in CA	4.0	7.8
Overall Continuing Assessment for Civilian Personnel	3.9	7.6
Security Office Training in CA	3.7	8.3
Indicators of CA Program Effectiveness	3.6	7.2
Security Counseling (related to CA)	3.6	7.7
Inspections/Staff Assistance Visits (related to CA)	3.4	7.6
Employee Assistance Programs	3.3	7.9
Performance Appraisal Info. (related to CA)	1.4	6.2
Incentives for Reporting Derogatory Info.	0.8	6.0

Notes.

The scale used ranged from "0" (Not used) to "10" (Very effective).
The sample sizes for these analyses ranged from 35 to 42.

Table 17

Mean Ratings by Army, Air Force, and Navy Collateral Installation Security Managers of the Current and Potential Effectiveness of Various Continuing Assessment Program Components

Continuing Assessment (CA)	Mean Current Effectiveness			Mean Potential Effectiveness		
Program Component	Army	AF	Navy	Army	AF	Navy
Clearance Suspension/Revocation Process	6.2	7.2	6.6	8.5	9.1	7.7
Sources of Derogatory Information	5.9	5.9	5.7	9.0	9.1	8.2
Service Branch CA Regulations	5.1	5.7	6.1	9.4	7.6	8.4
Indicators of Security Risk	6.1	4.8	5.2	8.5	7.9	8.0
Overall Continuing Assessment for Military Personnel	5.3	5.4	4.9	8.6	8.5	8.3
CA Reporting Procedures	4.9	5.2	4.8	8.8	8.1	7.8
Security Education (related to CA)	5.5	5.1	4.4	8.1	9.0	8.1
Security Briefings (related to CA)	5.3	4.6	4.9	7.9	8.0	7.8
DoD Security Regulations	6.1	3.9	4.2	9.1	4.9	7.2
Local CA Regulations	4.9	5.4	3.7	7.3	7.5	8.4
CA Recordkeeping Procedures	4.7	5.1	4.0	8.6	7.9	6.8
Coordination of CA Information With Other Groups	4.4	4.4	3.0	9.1	7.5	7.0
Unit Security Staff Training in CA	4.4	4.9	1.1	7.5	8.4	7.0
Overall Continuing Assessment for Civilian Personnel	4.0	4.0	3.7	6.9	8.1	8.1
Security Office Training in CA	3.4	4.6	3.1	8.3	8.9	7.7
Indicators of CA Program Effectiveness	4.9	3.9	1.9	8.4	6.6	6.6
Security Counseling (related to CA)	3.5	3.4	3.9	7.6	7.6	7.9
Inspections/Staff Assistance Visits (related to CA)	4.1	3.9	1.8	7.6	8.2	6.8
Employee Assistance Programs	2.5	3.9	3.8	8.3	7.7	7.6
Performance Appraisal Info. (related to CA)	0.6	2.3	1.5	7.1	5.9	5.6
Incentives for Reporting Derog. Info.	0.6	1.4	0.5	6.2	6.9	4.8

Notes.

The scale used ranged from "0" (Not used) to "10" (Very effective).
The sample sizes for these analyses were Army (13 to 15), Air Force (13 to 15), and Navy (6 to 13).

Security managers rated the overall effectiveness of current continuing assessment at 5.8 on a 10-point scale. In contrast, the mean rating of the effectiveness of periodic reinvestigations was 7.0.

Security managers were asked which aspects of the continuing assessment program are working best and which aspects are not working well. The results indicate that several of the same areas were mentioned in both lists. In other words, some of the areas which work well at some installations are not working well at other installations. Areas most frequently mentioned as working well include: reporting from installation departments (e.g., military police, personnel office, employee assistance, investigations office), coordination with the adjudication facility/headquarters, the clearance suspension/revocation process, security education and awareness procedures, security briefings, periodic reinvestigations, and reporting from unit personnel (e.g., coworkers, supervisors, unit commanders, and unit security managers), and procedures for reporting security information. Areas most frequently cited as not working well include: cooperation and reporting from installation departments, security education and awareness procedures, cooperation and reporting from unit personnel, and coordination with the adjudication facility/headquarters and the clearance suspension/revocation process, and procedures for reporting security information.

When asked what the most important factor is in the development of an effective continuing assessment program, the majority of respondents cited security education and awareness. Other major themes included having adequate program resources, obtaining cooperation from derogatory information reporting sources, and having good continuing assessment regulations.

Report 4 of this series (Bosshardt, DuBois, & Crawford, 1991b) provides an extensive discussion of this and other general issues related to the overall personnel security program.

Other Survey Topics

This section briefly discusses two additional topics included in the security manager interview protocol--information from employee assistance groups and security counseling. Each topic is discussed separately below.

Information from employee assistance groups. One concern for security managers was obtaining security-relevant information from employee assistance groups. When asked what security-information employee assistance programs have that the security office does not have access to, respondents most frequently cited medical, mental health, family, alcohol, drug, and financial information. Other types of information mentioned included criminal records and sexual misconduct.

Ideas frequently mentioned for encouraging employee assistance personnel to share security-related information with the security office included increasing security education, awareness, and training in continuing assessment, and incorporating continuing assessment in employee assistance group regulations. Additional suggestions included developing a standard reporting form for employee assistance personnel, establishing memoranda of agreement which define the types of information to be shared, mandating the sharing of information, and increasing communication between the security office and employee assistance groups.

Security counseling. The DoD and DCI regulations which govern continuing assessment procedures encourage installations to provide security counseling for individuals with problems that might have a bearing on their clearance status. Approximately 70 percent of the collateral sites and all of the SCI sites surveyed provide security counseling for individuals who have personal problems that might have a bearing on their eligibility for a security clearance or access. However, when asked whether individuals who provide this counseling typically have an extensive background and knowledge of the vulnerabilities for the type of security-related matter involved, only 49 percent of the collateral site respondents answered "yes." Additionally, only 45 percent of the respondents suggested that supervisors are generally aware of when and how to refer individuals for security counseling.

The most common suggestions for improving security counseling as it relates to continuing assessment were to educate and train persons who provide counseling, to increase security education, and to advertise that security counseling exists. Other suggestions to improve counseling included having staff or top management personnel provide security counseling and making it mandatory for those persons who are the subjects of reports of derogatory information.

SECTION 6: COMPARISONS OF THE SURVEY RESPONSES FOR DIFFERENT GROUPS

This section compares the survey responses of several groups of respondents. Discussions with field personnel suggested six factors which could affect the survey responses. These were: (1) level of access (SCI vs. collateral), (2) service branch (Army vs. Air Force vs. Navy), (3) geographic location (U.S. vs. overseas), (4) personnel type (civilian vs. military), (5) respondent type (security manager vs. unit security manager vs. unit commander), and (6) respondent tenure (longer term vs. shorter term).

The first four factors may affect the nature or effectiveness of continuing assessment programs due to differences in either the nature of the security threat or in the organizational structure. The final two factors, which are characteristic of the survey respondents, could yield differences in survey results because of their differing perspectives on the nature of continuing assessment programs.

An awareness of differences between groups is essential for at least three reasons. First, knowledge of these differing contexts and types of respondents is important for interpreting the survey results. Second, such knowledge is necessary for understanding the extent to which policy and procedural changes can be made across DoD organizations, as opposed to changes which must be tailed to specific groups. Finally, understanding these differences is essential to identify which factors differentially impact the effectiveness of operational continuing assessment programs.

In order to assess the general level of agreement between the responses provided by different groups, correlations were computed between the group profiles of mean item ratings for continuing assessment problems and recommendations. These correlations are shown in Table 18.

The results in Table 18 indicate that the correlations between the mean 136-item problem profiles for various groups range were consistently high, ranging from .71 to .86. This suggests there was very high general levels of agreement between these different groups with respect to their perceptions of the obstacles in maintaining a highly effective continuing assessment program.

Table 18 also presents the correlations between the mean 143-item recommendation item profiles for different groups. These correlations range from .57 to .78. Although slightly lower than the correlations on the problem items, these correlations still suggest high overall general

Table 18

Correlations Between Mean Problem and Recommendation Item Profiles of Selected Groups

Comparison Groups	Problem Items	Recommendation Items
1. Collateral and SCI	.79	.70
2. Air Force and Army	.86	.71
Air Force and Navy	.76	.63
Army and Navy	.72	.57
3. U.S. and Overseas	.84	.67
4. Civilian and Military	.84	.68
5. Unit Security Manager and Unit Commander	.85	--
Unit Security Manager and Security Officer	.82	--
Security Officer and Unit Commander	.71	--
6. Short and Long Tenure Security Officers	.79	.78

Note. Unit commanders and unit security managers did not rate the recommendation items. Thus, no correlations for recommendations are reported for these comparisons.

Security education. Differences in security education between collateral and SCI programs were generally minor, but collateral security staff consistently cited greater difficulties in this area. When rating security education, there was a trend for security managers at collateral facilities to rate their personnel lower in the area of understanding their continuing assessment responsibilities than did SCI staff. Collateral personnel consistently gave greater emphasis to a number of difficulties associated with security education, such as inadequate instructions for completing forms, insufficient security education and briefings, and inadequate training on continuing assessment for supervisors and cleared individuals than SCI personnel. In the security education area, SCI personnel receive comparatively more specific information on local security threats. The results also indicate that SCI staff provide more and better security counseling and employee assistance to cleared individuals than do their collateral counterparts, and that SCI supervisors are more likely to know when and how to refer individuals for assistance.

Training for security personnel. Collateral respondents rated the quality of training for both installation and unit security staff higher than did SCI personnel.

Derogatory information sources and methods. SCI and collateral personnel emphasized different sources for gathering security-relevant information. SCI security representatives rated unit personnel (unit commanders, supervisors, first sergeants, subjects) as the most useful sources of security-relevant information; collateral site respondents gave top ratings to the central adjudication facility, the police blotter, and the investigations office. This differing emphasis may be the result of three factors: (1) fewer numbers of cleared personnel in SCI facilities compared to collateral facilities (e.g., the median number of personnel covered in SCI continuing assessment programs was 1027 vs. 2208 for collateral sites), (2) greater personnel resources are devoted to continuing assessment (e.g., on average, there are three SCI security managers vs. one collateral security manager, per 1000 cleared personnel; also, 29 percent of SCI unit security manager time is devoted to continuing assessment vs. 14 percent for collateral sites), and (3) increased acceptance of and cooperation with security activities by personnel in SCI environments. With fewer resources to monitor a larger group of cleared individuals, collateral security staff apparently place greater emphasis on indirect sources where information is already gathered and recorded.

A few differences emerge in the outcomes for SCI and collateral continuing assessment programs. For example, the types of derogatory incidents reported differed somewhat for SCI and collateral personnel. Security violations and foreign travel/associations were reported more frequently at collateral sites than at SCI sites. Criminal felonies and court martials were reported relatively more frequently for collateral personnel than at SCI installations. Clearance suspensions were approximately twice as frequent per 1000 cleared individuals for collateral personnel compared to SCI personnel. The frequency of clearance revocations per 1000 cleared individuals was about the same for each group. Again, these frequencies are based on estimates provided by field security personnel.

Adjudication process. Both SCI and collateral personnel rated difficulties with the central adjudication facility as a top priority. SCI personnel, however, indicated greater difficulties with the clearance suspension and revocation process. These difficulties included the reluctance of unit personnel to report derogatory information because of its negative impact on unit effectiveness. SCI respondents (compared to collateral personnel) indicated, for example, a greater fear of having personnel lose access, more difficulties in obtaining replacement personnel in a timely manner, more problems associated with the amount of time taken for adjudication, and more concerns that the central adjudication facility does not take seriously enough the recommendations of the installation and unit commanders. This higher level of concern may reflect the more central role that clearances have for accomplishing work in an SCI environment.

Accountability. Collateral personnel cited a greater need for more inspection time on continuing assessment and suggested that incentives for performing continuing assessment duties have greater potential for contributing to increased program effectiveness. While SCI and collateral personnel have only partially implemented performance reviews for unit commanders on continuing assessment duties, SCI personnel are more likely to have conducted these reviews (e.g., 33 percent vs. 8 percent).

Differences in recommendations. Comparing the recommendations made by collateral and SCI personnel revealed some distinct differences. In general, collateral personnel placed greater emphasis on two areas--improving security indicators and improving security education. Collateral personnel gave higher ratings than their SCI counterparts to the following security indicators: (1) improving indicators for identifying individual and group security risk, (2) improving indicators of effective security performance, and (3) assessing the effectiveness of the continuing assessment program at each organizational level. Collateral personnel were also more likely to cite the need for improving the quality and frequency of security education. Much higher ratings were given by collateral personnel to the following items: improving security training and briefings for cleared personnel, ensuring that sources are familiar with their continuing assessment responsibilities, developing manuals or training modules to instruct personnel in how to complete the reporting forms, and increasing the number of security education personnel. Other items rated much higher by collateral personnel than by SCI personnel were to improve derogatory information report forms, to implement a derogatory information hotline at each installation, to reduce the number of persons with clearances and with access to classified information, to make supervisors more accountable for continuing assessment, and to have better access to the records of installation departments.

SCI personnel, in contrast, gave higher ratings to improving access to derogatory information than did collateral personnel. They emphasized the need for greater access to records and information held by the central adjudication office, the security police (i.e., the police blotter), the investigations office, and employee assistance groups. In addition, SCI personnel gave higher ratings to reducing unit disruption due to clearance suspensions/revocations, and to improving the counseling and assistance given to individuals who have security-related problems.

Differences Among Service Branches

Consistent with other group comparisons, survey responses for Army, Air Force, and Navy personnel are very similar. The few differences that emerged tend to be associated with the needs of the Navy (which most recently moved to central adjudication of personnel security clearances). These and other differences are briefly discussed below.[10]

Security education. Navy and Air Force personnel cited somewhat greater difficulties in the area of security education than did Army personnel. Specifically, the survey results indicated that (1) several continuing assessment topics (security risk indicators, reporting procedures, security threats) are not covered as thoroughly in Navy security education programs as in other services; and (2) a smaller percentage of Navy personnel receive refresher briefings addressing continuing assessment issues than in other services. Possible reasons for this are that Navy security staff members generally had less job tenure (in years, Navy = 2.3, Air Force = 3.6, Army = 7.1) and less experience in personnel security (Navy = 7.0, Air Force = 7.5, Army = 11.5) than Army or Air Force security office staff members. The Air Force had the lowest percentage of cleared and non-cleared persons who participated in security education during the past 12 months.

Training for security staff. Navy respondents tended to rate the quality of training for command and unit security staff representatives lower than did Air Force or Army respondents.

Derogatory information indicators, sources, and methods. The sources and types of reported derogatory information are highly similar across the services. The top five ranked sources of security information, in terms of usefulness, were nearly identical across the service branches. However, the order of rated importance for these sources does vary. The central adjudication facility and unit commanders were the most useful sources for Army security staff. The security police blotter and police personnel were the top ranked sources for the Air Force. Supervisors and the investigations office were the highest ranked sources for the Navy.

The most common types of reported derogatory incidents are relatively similar across the services. Alcohol abuse, drug abuse, and disciplinary problems represented the top three categories of reported incidents for each service. The fourth category was falsification of information for the Army, felonies for the Air Force, and financial problems for the Navy.

Adjudication process. It is interesting to note that although the Army and Air Force have used a system of central adjudication for many more years than the Navy, respondents in both services gave higher ratings than Navy respondents to several problems associated with the central adjudication process. Compared to Navy security staff, Army and Air Force respondents

[10] Appendix F provides several summary tables of the quantitative interview results for the service branches.

placed greater emphasis on difficulties in obtaining access to central adjudication personnel, insufficient use of tracers to update information, and problems resulting from long delays in adjudication decisions.

Accountability. In comparison to the other services, Navy respondents reported that less attention was given to procedures for ensuring accountability for continuing assessment. For example, the results indicated that Navy sites spend comparatively less time on inspections addressing continuing assessment activities and prepare fewer periodic reports on continuing assessment activities. All service branches reported very little use of performance reviews in the area of continuing assessment.

Differences in recommendations. Overall, the recommendation priorities of each service were very similar. Each service branch, however, placed greater emphasis on certain recommendations. Army respondents gave comparatively greater emphasis to increasing the entry and ceiling grade levels for security managers and to conducting an annual national agency checks on cleared individuals. Navy personnel gave more emphasis to the needs for: increased inspections addressing continuing assessment issues, improved training and security awareness, ensuring that central adjudication facility reviews files for security relevance before purging information, improving security counseling, improving initial clearance screening procedures, using more alternative sources of derogatory information, and ensuring that replacement personnel for persons who lose clearances are available in a timely manner. Air Force personnel gave greater emphasis to: encouraging unit commanders to report derogatory information to the security office, reducing clearance adjudication processing time, creating a full-time position for personnel security managers, conducting periodic checks of installation records, and instituting penalties for those who fail to submit continuing assessment paperwork.

Differences Between U.S. and Overseas Sites

Differences between U.S. and overseas continuing assessment programs are important to the extent that there are differential security threats or personnel vulnerabilities. Where significant differences exist, it is important to assess whether resources should be reallocated to meet the increased threats. For example, the survey results indicated that overseas security personnel devote more time to continuing assessment activities. If this corresponds to an increased security threat, this increased priority for continuing assessment is probably appropriate. On the other hand, the survey results indicated that more experienced personnel security staff tend to work in the U.S. This disparity may need to be examined.

Overall, the descriptions of continuing assessment programs for overseas and U.S. installations are very similar. These groups, however, did show minor differences in six areas: security education; training for security staff; derogatory information indicators, sources, and methods; accountability for continuing assessment; emphasis on continuing assessment; and program results. Each area is discussed separately below.

Security education. The survey results indicated that a smaller percentage of overseas personnel received security education in the past 12 months compared to U.S. personnel (54 percent vs. 73 percent for cleared personnel; 31 percent vs. 56 percent for non-cleared personnel). In contrast, overseas security staff reported that, on average, a greater percentage of briefing time is devoted to continuing assessment (61 percent vs. 28 percent for initial briefings; 54 percent vs. 32 percent for refresher briefings). These findings suggest that overseas security staff give more emphasis to continuing assessment, but for whatever reasons, overseas personnel do not participate as often in continuing assessment as do personnel at U.S. installations.

Training for security staff. Overseas respondents generally rated the quality of training for both installation and unit security staff members higher than did U.S. respondents.

Derogatory information indicators, sources, and methods. U.S. and overseas personnel use essentially the same sources for gathering derogatory information. The central adjudication facility was the most highly rated source for both groups. Overseas personnel, however, gave higher rankings to first sergeants, military police, and to the legal department than did U.S. personnel. Overseas Army personnel in particular rated the legal department as a highly useful source of derogatory information.

Examination of the types of derogatory incidents reported indicates a trend toward an increased vulnerability for overseas personnel. The estimates provided by installation security managers suggested that overseas personnel were much more likely to be involved in alcohol abuse, security violations, and mental/emotional difficulties than U.S.-based personnel. Reported incidents of sexual misconduct, financial problems, and criminal felonies were also somewhat higher for overseas personnel. This pattern suggests that overseas personnel are more likely to experience significant adjustment problems and have security-related problems.

In other findings, overseas personnel rated the complexity of reporting forms, the fact that some units are not covered by the installation continuing assessment program, and cooperation from local civilian authorities and from U.S. federal agencies as greater problems than did U.S. personnel; in contrast, U.S. personnel more frequently cited the lack of automation of the police blotter as a problem. Overseas respondents were also less likely to prepare reports related to continuing assessment.

Accountability. Overseas personnel reported a substantially greater amount of personnel security inspection time is devoted to continuing assessment (40 percent vs. 17 percent). In addition, continuing assessment was somewhat more likely to be included on performance reviews for overseas personnel than for U.S. personnel, although the overall percentage is quite low. The greater attention to accountability in continuing assessment for overseas personnel may reflect the perception of a greater security threat for overseas installations.

Emphasis on continuing assessment. U.S. personnel more frequently cited low grade levels of security personnel than did overseas respondents.

Differences in recommendations. The principal theme that distinguished U.S. and overseas priorities for improving continuing assessment is that greater emphasis is given by U.S.-based security managers to the improvement of reporting by various sources of derogatory information. U.S.-based personnel cited the need to better utilize a broad range of sources, including employee assistance, central adjudication, computer databases, previous commands, unit personnel, random drug testing, local authorities, and federal agencies. U.S. personnel also more strongly emphasized the need for more personnel security staff than did their overseas counterparts. In contrast, overseas personnel gave more emphasis to the importance of security awareness and commander accountability for continuing assessment.

Differences Between Military and Civilian Installations

Distinctions between installations with predominantly military or civilian personnel could have an impact upon the optimal methods for the effective implementation of a continuing assessment program. For example, there are fewer restrictions and controls on civilian personnel, a fact noted by security staff who often cited the difficulties this presents for gathering accurate and complete security-relevant information. An additional reason that might account for differences in the survey results between these two groups is that civilian installations surveyed tend to be research and development facilities, whereas the military sites surveyed are predominantly intelligence, training, and support facilities. The differences in the survey results are organized according to five topic areas: security education; derogatory information sources, methods, and indicators; accountability; and emphasis on continuing assessment.

Security education. Military and civilian installations were highly similar with respect to security education for cleared personnel and the training of personnel security staff members. The only significant difference found was that a higher percentage of refresher briefing time is devoted to continuing assessment by military installations.

Derogatory information indicators, sources, and methods. The primary area that distinguished civilian and military installations was the difficulty cited by respondents at civilian installations in obtaining security-relevant information. Survey respondents at civilian sites expressed greater concern about legal restrictions in gathering, recording, and reporting derogatory information. They also cited greater difficulties in obtaining information from employee assistance programs and from non-installation sources than did military personnel.

With respect to program outcomes, the top three types of derogatory incidents were identical for both types of installations: alcohol, drugs, and disciplinary problems. However, incidents of falsification of information occurred more frequently at civilian installations, whereas incidents of sexual misconduct occurred more frequently at military installations.

Ratings of the effectiveness of various continuing assessment program components were nearly identical for military and civilian sites. However, respondents at civilian sites gave indicators of security risk a higher effectiveness ranking, whereas respondents at military sites gave recordkeeping a higher effectiveness ranking.

Accountability. Security managers at military sites reported that a greater percentage of inspection time is devoted to continuing assessment in comparison to civilian sites (24 percent vs. 14 percent).

Emphasis on continuing assessment. Respondents at civilian sites expressed greater concerns over the grade levels for entry level and senior security managers than did respondents at military sites.

Differences in recommendations. Five themes characterize the differences in recommendation priorities between personnel at civilian and military installations. First, security personnel at civilian installations placed greater emphasis upon improving the entry and ceiling grade levels of security personnel. Second, personnel at civilian installations gave a much higher priority to improving security indicators (e.g., for security risk, financial difficulties, and for effective performance of security duties). Third, security personnel at military installations placed greater emphasis on making improvements in recordkeeping, citing the need to ensure that all relevant information is included in the files and that information is not removed, altered, or lost during transfers of individuals. Fourth, security personnel at military installations recommended more frequent inspections of records and that recordkeeping should be automated. Finally, respondents at military sites gave more emphasis to increasing the resources devoted to security (e.g., obtaining more computers, redirecting some resources from other areas to continuing assessment).

The four preceding sets of group comparisons examined dissimilarities in survey responses as a function of variations in the context of continuing assessment programs. The next two sets of group comparisons examine survey results with respect to differences in the respondents' perspective. First, we examine the alternative perceptions of continuing assessment as viewed by security managers, unit security managers, and unit commanders. Next, we examine the differing perceptions of highly experienced and novice security staff members.

Differences Across Types of Survey Respondents

Comparisons among different types of respondents provide useful information regarding the various needs and priorities of personnel with differing security and mission responsibilities. Obviously security managers, whose primary responsibility is to achieve security program objectives, will differ somewhat in their perception of problems and recommendations for continuing assessment from unit commanders, whose primary responsibilities concern mission accomplishment.

Overall, the results for security managers, unit commanders, and unit security managers were highly similar (see Table 18). Some of the major differences among these groups are presented below.

Compared to installation and unit security managers, unit commanders gave more emphasis to concerns which affect mission status. For example, unit commanders gave higher ratings than security staff members to difficulties associated with initial clearance procedures, inadequate tracers for updating clearance status, lack of additional emphasis to individuals with Top Secret access, and inadequate indicators of security risk. Not surprisingly, security managers and unit security managers rated the reluctance of commanders to report derogatory information as a greater problem than did unit commanders. Specifically, they noted that unit commanders are reluctant to report derogatory information because of the fear of losing a cleared person for long periods of time. In addition, both groups of security managers gave greater emphasis than unit commanders to including continuing assessment as a performance appraisal area for commanders.

Compared to security managers, unit commanders and security managers had more concerns about reporting forms (too complex), continuing assessment regulations (too complex), and the alteration or destruction of records relevant to continuing assessment. They also gave more emphasis to problems with central adjudication, especially in the area of delays caused by clearance suspensions.

Finally, security managers and unit commanders were more likely than unit security managers to emphasize the inadequacies of inspections.

No differences in responses across groups can be cited regarding recommendations for improving continuing assessment, as unit commanders and unit security managers did not rate these items.

Differences Between Longer-term and Shorter-term Security Personnel

Analyses were also conducted to examine whether there are consistent patterns of responses associated with the more in-depth knowledge of personnel security that may result from extensive job experience. Such patterns may indicate a consensus of expert opinion on important, yet subtle, continuing assessment issues. Where novice security staff members differ from experienced incumbents, training for novice security staff may be required.

The survey results suggest that experienced security staff place greater emphasis than novice staff on problems associated with (1) having some installation units which are not covered by the installation security office, (2) having inadequate performance reviews in the area of continuing assessment for commanders and supervisors, (3) having the service or transferring individuals destroy continuing assessment records, (4) understaffing the security office, (5) having insufficient penalties for falsifying security forms, and (6) having limitations regarding the types of derogatory information that can be obtained. In contrast, less experienced security staff gave more emphasis to difficulties with central adjudication (e.g., insufficient access to central adjudication personnel, inadequate use of tracers to update security information), the numbers of persons with clearances and access, inadequacies in security counseling, a lack of detail in the regulations, a lack of periodic record checks of installation department records, and a lack of resources (personnel, equipment) for continuing assessment.

Differences in recommendations. Experienced personnel gave greater emphasis than less experienced security personnel to increasing continuing assessment materials, redirecting some resources from other areas of security to continuing assessment, improving forms for reporting derogatory information, and increasing the minimum grade level for security staff members as a means of improving continuing assessment. Those with less experience gave more emphasis to the improvement of methods for gathering continuing assessment information (e.g., from unit commanders, other commands, employee assistance groups, other installation departments, and non-installation sources). Other more highly regarded suggestions by novice security managers included reducing the number of personnel with clearances and the amount of classified information, developing a security manual for unit security managers, and coordinating better with off-installation sources, developing better indicators, reducing difficulties with central adjudication (e.g., clearance processing time, lack of access), and developing better security risk indicators.

SECTION 7: SUMMARY

This report examined the continuing assessment of cleared personnel in the military services. The project involved three primary activities: (1) a review of regulations and literature related to continuing assessment, (2) a survey of Army, Air Force, Navy, and Marines Corps installations around the world to obtain detailed information about their continuing assessment programs, and (3) an analysis of systems issues related to continuing assessment.

This report is one of four project reports. It discusses the procedures and results of a large-scale survey of continuing assessment programs in the military services.

The initial step in this phase of the project involved a series of meetings with service headquarters and adjudication officials to gain an initial understanding of continuing assessment programs. Nine military installations were then visited to obtain an understanding of operational continuing assessment programs in the military and to gather information necessary for developing the research approach to be used during the survey.

Three survey forms were developed. These included an interview protocol for installation security office representatives and two shorter survey forms for unit security managers and unit commanders. The forms were developed on the basis of several inputs: results of the preliminary site visits, findings of the literature review, results of discussions with headquarters and adjudication personnel, reviews by continuing assessment experts, and a pilot test.

These survey forms were administered at 60 sites between September, 1989 and January, 1990. The survey sample included 21 Air Force, 19 Army, 18 Navy, and 2 Marine Corps sites. Forty-eight sites were collateral sites and 12 were SCI sites; ten sites were overseas sites. Overall, survey data were received from 60 installation security office representatives, 126 unit security representatives, and 88 unit commanders.

The survey yielded five types of data: (1) ratings of 136 problems by security managers, unit security managers, and unit commanders; (2) listings of the major problems encountered by security managers, unit security managers, and unit commanders; (3) ratings of 143 recommendation items by security managers; (4) listings of suggestions for improving continuing assessment from security managers, unit security managers, and unit commanders; and (5) structured interview data from security managers.

To facilitate the analyses and interpretation of the survey results, a taxonomy of continuing assessment problem/recommendation, or "finding," areas was developed. This taxonomy included eight general categories: (1) security education/briefings/awareness; (2) training for security personnel; (3) derogatory information indicators/sources/methods; (4) adjudication facility/process; (5) accountability for continuing assessment; (6) continuing assessment regulations; (7) emphasis on continuing assessment; and (8) continuing assessment system considerations.

Results of the survey analyses indicated that security education was the highest ranked of the eight continuing assessment taxonomy areas across all problem and recommendation data sets. Training for security personnel, continuing assessment system considerations, derogatory indicators/sources/methods, and the adjudication facility/process received moderate to high rankings across the various data sets. Continuing assessment regulations and accountability for continuing assessment received the lowest overall rankings.

Comparisons of the survey responses were also made according to six site/respondent characteristics: (1) level of access (SCI vs. collateral), (2) service branch (Army vs. Air Force vs. Navy), (3) geographic location (U.S. vs. overseas), (4) personnel type (civilian vs. military), (5) respondent type (security manager vs. unit security manager vs. unit commander), and (6) respondent tenure (longer term vs. shorter term). Results of these analyses indicated high levels of agreement among various groups. However, some differences in continuing assessment program emphases, procedures, problems, and recommendations did emerge and were discussed in the report.

The principal findings and recommendations from this survey are discussed in Report Three of this series (Bosshardt, DuBois, & Crawford, 1991a).

REFERENCES

Abbott, P. S. (1987). *Personnel security continuing evaluation (CE) programs* (FR 87-01). Alexandria, VA: HumRRO International, Inc.

Bosshardt, M. J., DuBois, D.A., & Crawford, K.S. (1991a). *Continuing assessment of cleared personnel in the military services: Report 3 - Recommendations.* (Tech Report PERS-TR-91-003). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M. J., DuBois, D.A., & Crawford, K.S. (1991b). *Continuing assessment of cleared personnel in the military services: Report 4 - System issues and program effectiveness.* (Tech Report PERS-TR-91-004). Monterey, CA: Defense Personnel Security Research and Education Center.

Crawford, K. S. (1988). *Continuing assessment in DoD: An overview. Proceedings of the Personnel Security Symposium.* Monterey, CA: Defense Personnel Security Research and Education Center.

Department of Defense. (1987). *Department of Defense personnel security program regulation* (DoD 5200.2-R). Washington, DC: Office of Deputy Under Secretary of Defense for Policy.

Director of Central Intelligence. (1986). *Minimum personnel security standards and procedures governing eligibility for access to sensitive compartmcntal information* (Directive No. 1/14, pp. 5-6).

DoD Security Review Commission, General Richard Stilwell (Chairman), (1985). *Keeping the nation's secrets: A report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices.* Washington, D.C.: Office of the Secretary of Defense.

DuBois, D.A., Bosshardt, M. J., & Crawford, K.S. (1991). *Continuing assessment of cleared personnel in the military services: Report 1 - A conceptual analysis and literature review.* (Tech Report PERS-TR-91-001). Monterey, CA: Defense Personnel Security Research and Education Center.

Fedor, B. (1988). *Introductory comments to the continuing assessment session. Proceedings of the Personnel Security Symposium.* Monterey, CA: Defense Personnel Security Research and Education Center.

General Accounting Office (1986). Information and personnel security: Data on employees affected by federal security programs. (GAO/NSIAD-86-189FS). Washington, D.C.: Author. (NTIS PB87-114849).

Glass, G.V., McGaw, B., & Smith, M. L. (1981). *Meta-analysis in social research.* Beverly Hills: Sage Publications.

Light, R., & Pillemer, D. (1984). *Summing up: The science of reviewing research.* Cambridge: Harvard University Press.

Secretary of the Army. (1986, November 25). Command security inspections--Action memorandum. Washington, D.C.: Author.

Secretary of the Navy. (1987, June 22). Lessons learned from command security inspections. Washington, D.C.: Author.

United States House of Representatives. (1988). *U.S. counterintelligence and security concerns: A status report-personnel and information security.* Report submitted by the Subcommittee on Oversight and Evaluation of the Permanent Select Committee on Intelligence. Washington, DC: U.S. Government Printing Office.

United States Senate. (1986). *Meeting the espionage challenge: A review of United States counterintelligence and security programs* (Report 99-522). Report submitted by the Select Committee on Intelligence, 99th Congress, 2nd Session. Washington, DC: U.S. Government Printing Office.

APPENDIX A:

Recommendations of Headquarters' Representatives For Improving Continuing Assessment

APPENDIX A

RECOMMENDATIONS OF HEADQUARTERS' REPRESENTATIVES FOR IMPROVING CONTINUING ASSESSMENT

Develop New Procedures for Gathering Derogatory Information on Cleared Personnel:

- Develop a questionnaire for security managers and commanders with questions about their awareness of (1) information that might affect someone's suitability of access, (2) letters of indebtedness for employees within the command, and (3) employees working extremely long office hours.

- Conduct random reinvestigations.

- Develop a security quiz (with questions such as "what would you do if ...").

Obtain Additional Derogatory Information on Cleared Personnel From Installation or Local Sources:

- Expand drug urinalysis testing (e.g., include civilians, test more frequently).

- Conduct local record checks and a medical check in additional to a National Agency Check.

- Obtain additional security-relevant information from the personnel office (e.g., have a personnel official review the employee's files for adverse information and inform the security office of relevant information).

- Obtain additional credit and local agency information on cleared individuals.

- Retain certain types of personnel records that are currently purged from DCII files after a predetermined period of time (e.g., letters of requirement, letters of caution).

- Increase use of the polygraph.

Obtain Additional National Agency Check (NAC) Information:

- Obtain NAC credit information for persons with SCI access.

- Conduct NACs on persons who possess secret sensitive information.

RECOMMENDATIONS OF HEADQUARTERS' REPRESENTATIVES FOR IMPROVING CONTINUING ASSESSMENT (cont.)

- Conduct NACs on contractors applying for SCI access who have been denied clearance/access at another agency.

- Conduct NACIs on all agency employees and send the security office a listing of individuals with unfavorable information.

Improve Security Education:

- Develop a universal security education training package.

- Conduct better security education and training.

Increase Commander Accountability for and Training in Continuing Assessment:

- Increase unit commander accountability for continuing assessment by increasing the penalties for not reporting derogatory information and including personnel security in the IG.

- Take actions that ensure the support of the installation and unit commanders for the continuing assessment program.

- Increase personnel security training for installation and unit commanders.

Improve Supervisor Accountability and Training in Continuing Assessment

- Have supervisors complete a continuing assessment form on each subordinate. This form would require endorsement or nonendorsement of several derogatory information items and the supervisor's signature.

- Increase supervisor accountability for continuing assessment by having the supervisor complete and sign a form on each subordinate certifying that the supervisor is or is not aware of derogatory information concerning the subordinate.

- Have supervisors evaluate whether an employee has met all security requirements three months before the employee is considered for a promotion.

- Have periodic supervisory briefings on continuing assessment topics.

- Increase continuing education for supervisors.

RECOMMENDATIONS OF HEADQUARTERS' REPRESENTATIVES FOR IMPROVING CONTINUING ASSESSMENT (cont.)

Include Continuing Assessment as a Performance Appraisal Area:

- Make continuing assessment an item on the supervisor's performance evaluation.
- Make the security category on the performance evaluation form more specific.

Include Continuing Assessment as a Part of the IG:

- Include continuing assessment in the IG.
- Include personnel security in the IG.

Examine the Personnel Reliability Program (PRP) for Ideas on Improving Continuing Assessment:

- Apply PRP requirements to improve accountability.
- Examine the criteria used for evaluating PRP when developing items for the continuing assessment survey.

Develop Continuing Assessment Regulation/Manual Supplements:

- Provide more detailed information regarding the implementation of the continuing assessment program.
- Develop an instruction booklet which explains how to complete the 398.

Miscellaneous Recommendations:

- Clarify the legal limitations in the continuing assessment process.
- Implement a nonpunitive amnesty program to increase self-reporting.
- Develop a psychological profile for access to a personnel security clearance.
- Redirect some of the resources devoted to initial clearance investigations to continuing assessment.
- Increase the size of the security staff.

RECOMMENDATIONS OF HEADQUARTERS' REPRESENTATIVES FOR IMPROVING CONTINUING ASSESSMENT (cont.)

- Perform a research study on known spies. This study would review the initial adjudication information on known spies, examine various derogatory information available, identify what continuing assessment tools might have been used, and examine the costs and benefits of different interventions.

- Conduct a research study which examines where security losses occur. More specifically, examine the actions of designated countries and identify those areas where they are making unexplained progress.

- Clarify the suitability vs. security criteria issue.

- Examine the feasibility of temporary access (so that the command can continue to carry out its operational missions).

APPENDIX B:

Continuing Assessment Survey Sites

APPENDIX B

CONTINUING ASSESSMENT SURVEY SITES

Army sites:

U.S. Army Missle Command
Anniston Army Depot
Fort McPherson
Watervliet Arsenal
U.S. Army Cold Regions Research Laboratory
Fort Devons
LABCOM
The Pentagon
U.S. Army Foreign Science and Technology Center
Fort Monmouth
Military Traffic Management Command
Fort Dix
Fort Bliss
White Sands Missile Range
Fort Huachuca
HQ EUSA
501st MI Brigade
WESTCOM Fort Shafter
66th MI Brigade Munich

Air Force sites:

Lackland Air Force Base
Kelly Air Force Base
Dyess Air Force Base
Scott Air Force Base
Peterson Air Force Base
Lowry Air Force Base
George Air Force Base
Norton Air Force Base
Vandenberg Air Force Base
Headquarters Space Division, Los Angeles Air Force Base
Patrick Air Force Base
Tyndall Air Force Base
Keesler Air Force Base
Wright-Patterson Air Force Base
Clark Air Force Base
Yokota Air Force Base
Hickam Air Force Base
Torrejon AB
RAF Mildenhall
Headquarters Electronic Security Command

CONTINUING ASSESSMENT SURVEY SITES (cont.)

Navy sites:

NAVSEAYSCOM
Naval Surface Warfare Center
USS Coral Sea (CV-43)
Fleet Intelligence Center-Europe and Atlantic
Naval Base Norfolk
Naval Air Station Miramar
USS Acadia (AD 42)
USS Okinawa (LPH-3)
Naval Submarine Base
Naval Security Group Activity, Northwest
Norfolk Naval Shipyard
NAVCOMMSTA Jacksonville
USS Luce (DDG-38)
U.S. Naval Station Subic Bay
U.S. Naval Air Facility, Atsugi, Japan
U.S. Naval Station, Rota, Spain
Navy Security Group Activity, Pearl Harbor
Fleet Intelligence Center, Pacific

Marine Corps sites:

Camp Pendleton
Kaneohe Marine Corps Air Station

APPENDIX C:

Mean Ratings for 136 Problem Items for All Respondents, Collateral Site Respondents, Unit Security Managers, and Unit Commanders

APPENDIX C

Mean Ratings For 136 Problem Items for All Respondents, Collateral Site Respondents, SCI Site Respondents, Security Managers, Unit Security Managers, and Unit Commanders

TAXON.[1] AREA	ALL	ALL COLLA- TERAL	ALL SCI	ALL SEC MGR	ALL UNIT SEC MGR	ALL UNIT CO	PROB- LEM NO.	PROBLEM ITEM TEXT
1 A	4.9	5.1	4.2	4.9	4.7	5.3	P- 91	CA sources are not familiar with their reporting responsibilities.
1 A	5.0	5.1	3.7	5.1	4.8	5.1	P- 87	Insufficient security education activities in the area of CA.
1 A	4.3	4.5	3.3	4.1	4.0	4.9	P-100	Inadequate refresher briefings on CA responsibilities.
1 A	4.3	4.5	3.1	3.7	4.2	4.8	P- 99	Inadequate initial briefings on CA responsibilities.
1 B	5.5	5.7	4.4	5.5	5.5	5.6	P- 89	Inadequate CA training for supervisors.
1 B	5.1	5.2	4.2	5.3	4.9	5.3	P- 88	Inadequate CA training for unit COs.
1 C	5.1	5.2	4.0	4.9	4.9	5.4	P- 90	Inadequate CA training for cleared individuals.
1 D	5.7	5.8	5.1	6.0	5.4	5.9	P- 94	Lack of trg modules to instruct COs/sup's on how to interpret security risk indicators.
1 D	5.6	5.7	4.9	5.6	5.5	5.7	P- 92	Lack of stan. trg modules for COs, sup's, cleared indl's which describe their CA duties.
1 D	5.2	5.3	4.7	5.4	5.1	5.2	P- 95	Lack of trg aids to assist supervisors in identifying high risk individuals.
1 D	5.1	5.2	4.5	6.1	4.8	4.9	P- 93	Lack of videotapes to train personnel in their CA responsibilities.
1 D	4.3	4.4	3.5	4.6	4.2	4.2	P- 96	Lack of adequate CA education materials from headquarters (eg, lessons learned, etc.)
1 D	3.4	3.7	1.8	3.6	3.3	3.5	P- 98	Lack of/inadequate instruction manuals or videotapes on how to complete security forms.
1 E	3.8	3.9	3.1	4.0	3.5	4.1	P- 97	Inadequate security awareness materials.
2 B	4.8	4.9	4.1	4.9	4.7	4.9	P- 84	Inadequate CA training for security officers.
2 C	5.0	5.1	4.4	4.8	5.0	5.2	P- 85	Inadequate CA training for unit security managers.
3 A	4.7	4.9	3.5	4.1	4.8	4.9	P-136	Little is known about derog. info on past spies & what CA tools could have been used.
3 A	4.4	4.4	4.5	4.4	4.3	4.7	P- 17	Inadequate indicators for identifying persons with financial problems.
3 A	4.1	4.1	3.8	3.7	3.8	4.7	P- 16	Inadequate indicators for identifying persons who are potential security risks.
3 A	4.0	4.1	3.3	3.8	3.6	4.7	P- 18	Inadequate indicators of effective personnel security performance.
3 A	3.8	4.0	3.1	3.5	3.4	4.7	P- 19	Inadeq. indicators for assessing security risk associated with particular work groups.
3 C	6.5	6.6	6.1	6.2	6.3	7.0	P- 68	Reluctance of individuals to self-report derogatory information.
3 C	4.8	4.7	5.5	5.5	4.4	5.0	P- 28	Drug & alcohol testing is too limited.
3 C	4.5	4.6	4.0	3.8	4.4	5.1	P- 76	No amnesty program exists to increase self-reporting of derogatory information.
3 C	4.5	4.4	5.1	4.4	4.7	4.1	P- 51	Reluctance of persons to report because of legal implications.

Mean Ratings For 136 Problem Items for All Respondents, Collateral Site Respondents, SCI Site Respondents, Security Managers, Unit Security Managers, and Unit Commanders (cont.)

3 C	4.0	4.1	3.8	4.3	3.9	4.0	P- 41 No formalized standard requirement for individuals to self-report derogatory info.
3 C	3.3	3.2	3.9	3.2	3.1	3.7	P- 39 The polygraph is underutilized in CA.
3 D	5.7	5.8	5.2	5.7	5.8	5.6	P- 67 Reluctance of co-workers to report derogatory information.
3 D	5.4	5.3	6.0	5.6	5.6	5.1	P- 52 Reluctance of persons to report derog. info. bec. of concern of hurting indl's career.
3 D	4.5	4.6	3.9	4.3	4.4	4.6	P- 24 Few incidents are reported except through the police blotter.
3 D	4.4	4.4	4.2	4.7	4.6	4.0	P- 71 No standard form for supervisors to monitor subordinates' security-relevant behavior.
3 D	4.4	4.3	5.1	4.6	4.7	3.9	P- 53 Reluctance of persons to report derog. info. bec. the work unit would be disrupted.
3 D	4.0	4.2	2.9	3.3	4.5	4.0	P-135 Little knowledge from other CA programs (eg. PRP) incorporated into the DoD CA program.
3 D	3.8	3.7	4.6	4.7	4.1	2.9	P- 49 Reluctance of unit cmdrs to report derog. info. bec. of fear of losing cleared person.
3 D	3.7	3.5	4.8	4.5	3.9	2.8	P- 50 Reluctance of COs to report derogatory info. because the individual might lose access.
3 D	3.0	3.1	2.6	2.8	3.0	3.2	P- 44 Inefficient procedures for reporting derogatory information to the security office.
3 D	2.6	2.7	2.1	2.1	2.6	3.0	P- 42 Burdensome CA reporting requirements.
3 E	5.0	5.2	4.3	5.0	4.6	5.8	P- 45 Lack of formal reporting procedures & written standards for personnel, legal, medical,
3 E	4.7	4.7	4.8	5.0	4.9	4.3	P- 48 Reluctance of units to report derogatory information to the security office.
3 E	3.6	3.7	2.8	4.1	3.1	3.8	P- 81 Inadequate CA information is received from employee assistance groups.
3 E	3.3	3.6	1.8	3.3	3.1	3.7	P- 47 When derog. info arises on employee, input not obtained from diff. install. groups.
3 E	3.5	3.6	2.4	4.0	2.8	3.9	P- 82 The security office has little/no access to employee assistance records.
3 E	3.5	3.5	3.3	2.9	3.3	4.3	P- 26 Periodic record checks of various installation files for derog. info are not performed.
3 E	3.4	3.5	2.9	3.9	2.8	3.8	P- 46 Installation security office is unable to obtain relevant CA information from depts.
3 E	3.3	3.3	3.4	3.1	3.1	3.8	P- 31 Investigations office does not report sufficient derog. info. to the security office.
3 E	2.6	2.5	3.2	1.8	3.1	2.5	P- 23 Military/security police blotter info is not readily available to sec. office.
3 F	5.4	5.4	5.5	4.6	5.7	5.7	P-117 Difficulties obtaining derog. info. on cleared personnel when they are off instan.
3 F	4.5	4.5	4.6	3.8	4.6	4.8	P- 54 Difficulties obtaining personnel security information from sources outside the base.
3 F	4.4	4.4	4.5	3.9	4.5	4.7	P- 34 Other commands provide little/no CA information on cleared personnel.
3 F	4.3	4.4	3.6	4.6	4.0	4.6	P- 30 Relevant financial on cleared individuals is not provided to the security office.
3 F	4.0	4.1	3.6	4.0	3.8	4.4	P- 27 Relevant computer databases are not used for obtaining derogatory information.
3 F	4.0	4.0	4.0	3.3	4.0	4.6	P- 60 Local security office has little/no access to centralized derog. info. records.
3 F	3.8	3.9	3.1	3.4	3.6	4.3	P- 33 Information sources outside the base/command are rarely used.
3 F	3.6	3.6	3.5	2.6	3.9	4.0	P- 55 Inadequate communication between HQ and field personnel on CA.
3 F	3.4	3.4	3.5	3.0	3.5	3.9	P- 37 Derog. information hotlines are not used/fully utilized to obtain derog. info.
3 F	3.4	3.4	3.2	3.0	3.9	3.1	P- 38 Alternate sources are not fully utilized.
3 F	3.0	3.1	2.3	2.9	2.7	3.4	P- 29 NACs are not fully utilized as part of the CA process.
3 F	3.1	3.0	3.5	3.1	3.0	3.2	P- 36 Local civilian authorities are reluctant to provide derog. info. on cleared ind'ls.

Mean Ratings For 136 Problem Items for All Respondents, Collateral Site Respondents, SCI Site Respondents, Security Managers, Unit Security Managers, and Unit Commanders (cont.)

3	F	3.0	2.9	3.5	3.2	2.8	3.2	P- 35	Criminal record information is not obtained from federal agencies (FBI,etc).
3	F	2.7	2.7	3.2	2.7	2.5	3.1	P- 32	Silent listening posts are not used/fully utilized to obtain derogatory information.
3	G	4.2	4.3	3.4	3.8	3.9	4.9	P- 59	Lack of a centralized computer-automated records facility containing all CA records.
3	G	3.5	3.7	2.7	2.5	3.5	4.4	P- 61	Destruction of CA relevant records by the service.
3	G	3.0	3.2	1.9	2.6	2.8	3.6	P- 58	Relevant CA info is not entered into an individual's files.
3	G	3.0	3.0	2.7	2.1	3.2	3.6	P- 62	Alteration or destruction of CA relevant records by cleared ind'ls when they transfer.
3	G	2.8	2.9	2.2	2.1	2.9	3.2	P- 57	Burdensome CA paperwork requirements.
3	G	2.4	2.5	1.5	2.1	2.3	2.7	P- 43	Lack of/inadequate forms for reporting derog. info.
3	G	2.2	2.2	1.7	1.0	2.5	2.6	P- 56	Lengthy and complex CA forms.
3	G	2.1	2.1	2.2	1.3	2.6	2.1	P- 25	Military/security police blotter is not automated.
4	A	6.5	6.3	7.2	5.8	6.4	7.0	P-110	Too much time is taken by central adjudication facility to make clearance decisions.
4	A	5.5	5.4	6.4	4.6	5.3	6.4	P-127	Delays in obtaining replacement personnel for individuals who lose security clearances.
4	B	5.1	5.1	5.1	4.7	4.8	6.0	P-111	Security office has insufficient access to central adjudication office.
4	B	4.5	4.4	5.4	3.6	4.4	5.4	P-113	Inadequate/no tracers are used for updating base on an individual's clearance status.
4	B	3.3	3.2	3.6	2.9	3.0	4.0	P- 40	Central adjudication agency does not provide security office with suff. derog. info.
4	B	3.3	3.1	4.5	2.6	3.3	3.9	P-112	Central adjudication does not take seriously enough the recommendations of base/unit CO
4	B	2.6	2.6	2.7	2.3	2.7	2.7	P-125	Installation does not have clearance determination authority.
4	B	2.3	2.3	1.9	1.7	2.4	2.5	P-126	Unit cmdrs can't grant access to cleared individuals who are under investigation.
5	A	4.3	4.4	3.8	4.7	4.3	4.1	P- 66	Supervisors are not held accountable for failing to carry out their CA responsibilities
5	A	3.3	3.4	2.8	4.1	3.2	2.9	P- 64	Unit COs are not held accountable for failing to carry out their CA duties.
5	A	2.8	2.9	2.3	2.8	2.9	2.7	P- 63	Installation commander is not held accountable for deficiencies in CA program.
5	B	4.8	4.9	4.4	5.2	4.7	4.7	P- 73	Few or no consequences for failing to comply with CA reporting requirements.
5	B	4.4	4.5	3.9	4.2	4.7	4.2	P- 72	Lack of rewards for persons who are extremely conscientious in performing CA duties.
5	B	4.3	4.4	3.7	4.4	4.4	4.1	P- 75	Few or no penalties for failing to submit required PR paperwork before the 5 year limit
5	B	3.9	4.0	3.2	3.7	3.9	4.1	P- 74	Insufficient penalties for falsifying security forms.
5	C	4.4	4.5	3.8	5.2	4.6	3.6	P- 69	Personnel security is not always included as a performance evaluation item for unit COs
5	C	3.7	3.8	3.0	3.2	3.6	4.1	P-134	Inadeq. knowledge of behaviors that differentiate effective/ineffective security mgrs.
5	C	3.3	3.4	3.2	3.3	3.7	2.9	P- 70	Vague wording of the security item on the performance evaluation form.
5	D	3.5	3.6	3.1	4.2	3.1	3.6	P- 77	Lack of/inadequate CA inspection checklists.
5	D	3.5	3.6	3.0	4.3	3.0	3.7	P- 78	Inadequate number/quality of CA inspections.
5	D	3.2	3.4	2.3	3.8	2.5	3.9	P- 79	CA is not included in command inspections.
5	D	2.9	3.1	1.9	3.4	2.2	3.5	P- 80	CA is not included on the IG.
5	E	4.8	5.0	3.8	4.6	4.6	5.1	P-102	Lack of knowledge regarding which aspects of CA are most effective.

Mean Ratings For 136 Problem Items for All Respondents, Collateral Site Respondents, SCI Site Respondents, Security Managers, Unit Security Managers, and Unit Commanders (cont.)

5	E	4.6	4.7	3.8	4.8	4.5	4.7	P-101	Inadequate indicators for assessing the effectiveness of CA at each reporting level.
6	A	3.6	3.7	3.1	3.8	3.5	3.7	P- 12	CA regs are poorly organized.
6	A	3.7	3.7	3.9	4.4	3.6	3.2	P- 10	CA regulations lack sufficient detail.
6	A	3.0	3.0	3.6	2.7	3.0	3.3	P- 15	Lack of a standard security regulation or manual for unit security managers.
6	A	2.8	2.9	2.2	2.3	2.8	3.4	P- 11	CA regs are too complex.
6	A	2.8	2.8	2.5	3.2	2.7	2.7	P- 14	CA regs limit the types of derogatory information that can be obtained.
6	A	2.8	2.7	3.6	2.5	2.8	3.2	P- 13	CA regs are inconsistent.
7	A	4.2	4.2	3.8	4.9	4.1	3.8	P-124	Top levels/senior executives of the service do not consider CA a top priority.
7	A	3.8	3.8	4.0	3.5	3.8	4.0	P-121	Operational readiness priorities adversely affect CA.
7	A	3.3	3.3	2.9	3.2	3.4	3.1	P- 65	Unit commanders are not sufficiently involved in the clearance determination process.
7	A	2.7	2.7	2.7	3.2	2.9	2.2	P-123	Installation commander does not properly emphasize CA.
7	A	1.9	1.8	2.3	1.6	1.9	2.0	P-122	Security officers lack access to the installation commander.
7	B	4.0	4.1	3.6	4.3	4.0	3.8	P- 8	Insufficient resources/effort are devoted to CA compared to other security functions.
7	B	3.8	3.9	3.3	3.4	3.7	4.2	P- 9	Insufficient resources/effort are devoted to CA compared to PRs.
7	B	3.3	3.3	3.0	3.8	2.8	3.4	P- 1	Inadequate funding for CA.
7	B	2.7	2.7	2.6	3.5	2.6	2.3	P- 7	Insufficient equipment for CA.
7	C	5.1	5.2	4.8	5.6	5.2	4.8	P- 4	*Insufficient time for unit sec. mgrs.* to peform their CA responsibilities.
7	C	5.0	5.0	4.7	6.0	4.8	4.7	P- 2	Understaffing of the personnel security office.
7	C	4.7	4.8	3.8	4.8	4.9	4.3	P- 5	Too many part-time security managers vs having fewer spend more time.
7	C	4.6	4.7	3.3	5.2	4.5	4.2	P- 86	Insufficient number of security education personnel.
7	C	2.8	2.8	2.8	2.0	3.0	3.1	P- 3	Insufficient number of unit security managers.
7	D	4.8	5.0	3.8	5.1	4.7	4.7	P-106	Lack of a separate, full-time position for personnel security officers.
7	D	4.9	4.9	4.4	4.4	5.0	5.0	P- 6	Inexperienced unit security managers.
7	D	4.4	4.4	4.7	4.4	4.2	4.8	P-119	Rapid turnover of cleared population.
7	D	4.2	4.2	4.1	4.2	4.2	4.2	P-103	Low grade level of security officers reduces the attractiveness of this career field.
7	D	4.2	4.2	4.4	4.2	4.1	4.3	P-104	Low grade level ceiling for senior security officers.
7	D	3.3	3.4	3.3	3.1	3.4	3.4	P-105	Failure to set a minimum grade level for unit security managers.
8	A	5.3	5.3	4.9	4.5	5.4	5.7	P-116	Difficulties obtaining derogatory information on civilians.
8	A	4.1	4.1	4.5	3.9	4.0	4.4	P- 22	CA procedures are not targeted to those at greatest security risk.
8	A	3.8	3.9	2.8	3.2	3.3	4.8	P-120	Ind'ls with TS access do not receive more CA emphasis than ind'ls with secret access.
8	A	3.2	3.2	2.8	3.0	3.1	3.5	P- 83	Inadequate counseling/assistance for cleared individuals with security problems.
8	B	4.5	4.4	4.8	4.2	4.6	4.5	P-133	The CA programs of the services differ and should be consolidated into a single program
8	B	4.3	4.3	4.3	4.2	4.7	3.9	P-128	Poor attitude towards personnel security among base personnel.

Mean Ratings For 136 Problem Items for All Respondents, Collateral Site Respondents, SCI Site Respondents, Security Managers, Unit Security Managers, and Unit Commanders (cont.)

8 B	3.5	3.6	3.2	3.1	3.5	3.9	P-129	Special accesss programs create confusion and excess burdens on unit security managers.
8 B	1.8	1.8	2.1	1.8	1.8	1.9	P-131	Some units on the installation are not covered by the installation CA program.
8 C	5.0	5.0	4.7	4.3	5.2	5.3	P-114	Existing laws/privacy restrictions make it difficult to obtain CA info. on civilians.
8 C	4.7	4.8	4.4	3.8	5.0	5.1	P-115	Legal concerns constrain the reporting and documentations of derogatory information.
8 D	5.1	5.0	5.5	4.9	5.0	5.3	P-118	Difficulties monitoring large numbers of cleared personnel.
8 D	4.9	4.9	4.9	3.8	5.1	5.4	P-109	Too much classified information is produced.
8 D	4.2	4.3	3.3	4.4	4.1	4.1	P-107	Too many persons have security clearances.
8 D	4.0	4.0	3.6	4.4	3.8	4.0	P-108	Too many persons require access to classified information.
8 E	4.2	4.2	3.9	3.6	3.9	4.9	P- 21	Failure to conduct random reinvestigations.
8 E	3.7	3.8	3.3	3.8	3.3	4.3	P- 20	Systematic CA information is gathered too infrequently.
8 F	4.1	4.1	4.1	3.8	4.2	4.1	P-130	Too many high security risk individuals receive clearances.
8 F	3.2	3.3	2.4	2.1	3.4	3.7	P-132	Inadequate procedures for det. whether individuals should receive initial clearance.
MEAN	3.98	4.03	3.67	3.87	3.92	4.16		
SD	0.93	0.94	1.04	1.08	0.94	0.9		

[1] See Table 6 for a listing of the taxonomy subcategories.

Note. Ratings were made on a "0" to "10" scale.

APPENDIX D:

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents

APPENDIX D

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents

TAXON.[1] AREA	ALL	ALL COLLA- TERAL	ALL SCI	ITEM NO.	RECOMMENDATION ITEM TEXT
1 A	7.1	7.4	5.9	R-101	Ensure derog. info sources are familiar with the CA responsibilities.
1 A	7.0	7.1	6.2	R- 97	Increase security education activities related to CA.
1 A	6.6	6.8	5.2	R-111	Conduct more/better refresher briefings on CA responsibilities.
1 A	6.5	6.7	5.7	R-110	Conduct more/better initial briefings on CA responsibilities.
1 B	7.4	7.6	6.4	R- 99	Improve CA training for supervisors.
1 B	7.2	7.3	6.5	R- 98	Improve CA training for unit commanders.
1 C	7.0	7.2	6.0	R-100	Improve CA training for cleared individuals.
1 D	7.5	7.5	7.3	R-103	Develop training modules to instruct cmdrs & sprvrs on how to spot security risk indicators.
1 D	7.1	7.3	6.0	R-104	Develop training aids to assist supervisors in identifying ind'ls who have security-related problems.
1 D	7.2	7.2	6.8	R-102	Develop standard training modules for unit cmdrs, supervisors, and cleared individuals.
1 D	6.3	6.4	5.8	R-106	Increase the number and quality of CA materials provided by headquarters.
1 D	6.2	6.2	5.8	R-107	Use more security awareness materials.
1 D	4.9	5.5	1.6	R-109	Develop instruction manuals, regs, or videos on how to complete security-related forms.
1 E	4.2	4.4	3.0	R-108	Promote security awareness by advertising on local radio and TV.
2 B	7.3	7.1	8.1	R- 94	Increase/improve CA training for security officers.
2 B	5.0	5.2	3.8	R-141	Identify effective and ineffective behaviors of sec offcrs to provide info for trg procedures.
2 C	7.1	7.1	7.1	R- 95	Increase/improve CA training for unit security managers.
3 A	6.2	6.5	4.7	R-143	Perform study on known spies examining what derog info was avail, what CA tools might have been used.
3 A	5.6	6.0	3.9	R- 16	Develop better indicators for identifying persons who are potential security risks.
3 A	5.8	5.8	5.4	R- 17	Develop better indicators for identifying persons with financial problems.
3 A	4.8	5.2	3.3	R- 18	Develop indicators of effective personnel security performance.
3 A	4.7	5.0	3.0	R- 19	Develop indicators for assessing the security risk associated with particular work groups.
3 A	4.1	4.2	3.7	R- 48	Examine procedures which gather info on a subject's history of security responsibleness.
3 C	6.2	6.3	6.1	R- 28	Expand drug/alcohol testing.
3 C	6.0	6.1	5.2	R-142	Review other CA programs for ideas on improving CA.
3 C	5.5	5.7	4.8	R- 78	Take actions which encourage individuals to self-report derog. info.
3 C	4.9	5.2	3.8	R- 86	Implement an amnesty program to increase self-reporting of derog. info.
3 C	4.7	4.9	3.6	R- 42	Have security officer...conduct in-depth interview with each ind'l (re)considered for a clearance.

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents (cont.)

3 C	4.7	4.8	4.1	R- 46	Have cleared individuals complete a questionnaire to identify persons with security-related problems.
3 C	4.6	4.7	4.2	R- 41	Have cleared individuals complete a derog. self-report form each year.
3 C	4.2	4.3	3.7	R- 39	Increase/initiate use of the polygraph for CA.
3 C	3.6	3.9	2.6	R- 44	Have cleared individuals periodically complete CA quiz as a req't for obtaining a security clearance.
3 C	3.4	3.6	2.9	R- 47	Have cleared individuals complete a life events quest. to identify potential security risks.
3 C	3.4	3.6	2.4	R- 43	Have individuals pass a short quiz on CA as a req. for obtaining clearance.
3 C	3.3	3.5	2.3	R- 45	Conduct psychological testing to assess the potential security risk of individuals.
3 D	5.9	6.1	5.2	R- 77	Take actions which encourage coworkers to report derog. info.
3 D	6.1	6.1	6.1	R- 74	Take actions which encourage unit commanders to report more derog. info to the security office.
3 D	5.4	5.6	4.3	R- 75	Have unit cmdrs make an initial evaluation of ind'ls being considered for security clearances.
3 D	5.3	5.4	5.0	R- 81	Develop a stand. supervisory form for periodically evaluating security worthiness of subordinates.
3 E	7.3	7.1	8.0	R- 52	Dev. formal reporting procedures & standards...defining info to be shared with security office.
3 E	6.3	6.3	5.9	R- 54	Provide installation security office with more access to CA-relevant records kept by other bases.
3 E	6.0	6.2	4.9	R- 53	Develop a standard form for assessing an individual's security risk for use by ...staff...
3 E	6.4	6.2	7.4	R- 91	Have employee assistance personnel provide more derog. info regarding cleared individuals.
3 E	6.3	6.1	7.2	R- 58	Take actions which encourage units...to report more derog. info to the security office.
3 E	6.2	5.9	7.7	R- 92	Provide installation security office with greater access to employee assistance records.
3 E	5.9	5.7	7.3	R- 31	Have investigations office provide more derog. info to the security office.
3 E	5.3	5.5	4.1	R- 26	Conduct periodic checks of various installation dept. files for derog. info on cleared personnel.
3 E	5.3	5.4	4.5	R- 55	When derog. info arises on a cleared ind'l, require groups...to make a clearance recommendation.
3 E	5.5	5.4	6.0	R- 56	Have install. depts. which provide recommendations.. furnish more info to justify their decisions.
3 E	4.3	4.6	3.0	R- 57	Have personnel dept. gather CA info during regular info gathering points.
3 E	3.9	4.0	3.8	R- 23	Enter more security-relevant info onto the military/security police blotter.
3 F	6.7	6.4	8.3	R- 68	Provide local security personnel with more access to centralized derog. info records.
3 F	6.3	6.0	7.3	R- 30	Provide additional financial info to the security office.
3 F	5.9	6.0	5.1	R- 27	Use/increase use of computer databases to obtain derog. info on cleared individuals.
3 F	5.8	6.0	4.9	R- 62	Improve communication between headquarters and field personnel on CA matters.
3 F	6.2	6.0	7.2	R- 70	Ensure central adjudication facility reviews files for security info before any info is purged.
3 F	6.1	5.9	6.9	R-130	Obtain more derog. info on cleared individuals when they are off the installation.
3 F	5.5	5.4	5.8	R- 61	Develop better coordination with sources outside the military which possess security info.
3 F	5.1	5.1	4.6	R- 34	Increase the amt. of CA info obtained from an employee's previous command.
3 F	5.1	5.0	5.6	R- 33	Use more external sources of derog. info.
3 F	4.6	5.0	2.7	R- 37	Implement a "derog. info hotline" at each installation/command.

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents (cont.)

3	F	4.6	4.7	4.4	R- 29	Conduct annual or periodic NACs on all cleared ind'ls who are covered by the security office.
3	F	4.7	4.7	4.7	R- 36	Improve cooperation with local authorities on matters affecting employee security clearances.
3	F	4.7	4.6	5.2	R- 35	Obtain more criminal record info from federal agencies.
3	F	3.8	4.0	2.9	R- 38	Use more alternate sources of derog. info.
3	F	3.6	3.7	3.1	R- 32	Use/increase use of "silent listening posts" (informants) to obtain derog. info.
3	G	6.6	6.3	8.3	R- 69	Ensure CA records are not purged when individuals reenlist or transfer.
3	G	6.3	6.3	6.2	R- 71	Take actions to prevent cleared ind's from removing/altering copies of CA records when they transfer...
3	G	6.1	6.1	6.1	R- 65	Ensure all relevant CA info is entered into an individual's files.
3	G	5.6	5.9	4.2	R- 51	Improve procedures for reporting derog. info to the security office.
3	G	5.7	5.8	5.4	R- 67	Retain computer-automated records of all CA relevant info service-wide in a central repository.
3	G	4.5	5.1	1.8	R- 50	Improve derog. info reporting forms.
3	G	4.4	4.7	2.6	R- 49	Simplify CA reporting requirements.
3	G	3.7	3.8	2.9	R- 66	Create a security file for each cleared individual.
3	G	3.9	3.7	5.0	R- 25	Computer automate the military/security police blotter.
3	G	3.1	3.3	2.1	R- 64	Reduce CA paperwork requirements.
3	G	3.0	3.1	2.4	R- 63	Simplify and shorten CA forms.
4	A	6.7	6.6	6.9	R-121	Reduce the time required by adjudication facility for processing clearance suspensions/revocations.
4	A	5.5	5.4	6.5	R- 59	Reduce time required by investigations office for conducting investigations when derog info
4	A	5.7	5.4	6.9	R-137	Ensure replacement personnel are available in timely fashion for ind'ls whose clearances are revoked.
4	A	3.7	3.7	4.0	R-135	Provide installations with limited clearance determination authority.
4	A	3.6	3.7	3.4	R-136	Determine the feasibility of providing limited access to those under investigation.
4	B	6.9	7.1	6.0	R-123	Increase central adjudication facility phone lines/staff to provide more availability.
4	B	6.4	6.7	4.8	R-122	Increase the number of hours that the security office has access to central adjudication.
4	B	6.1	6.2	6.0	R-126	Use tracers for updating the installation/command on an individual's clearance status.
4	B	5.8	5.7	6.3	R-125	Have adjudication facil. provide cmdrs with more justification when cmdr's recommendation
4	B	5.2	5.1	5.4	R-124	Ensure adjudication facility gives more consideration to recommendations of installation/unit co...
4	B	4.8	4.4	6.9	R- 40	Ensure adjudication agency provides derog. info on cleared ind'ls to local security office.
5	A	6.1	6.4	4.9	R- 76	Make supervisors more accountable for reporting derog. info.
5	A	4.9	4.9	4.9	R- 72	Make installation commander more accountable for CA.
5	A	3.0	3.0	3.0	R-134	Require unit commanders to sign Form 398s (or 398-2s) rather than supervisors.
5	B	6.9	6.8	7.0	R- 84	Institute/enforce penalties for falsifying CA forms.
5	B	6.5	6.6	6.1	R- 85	Institute/enforce penalties for individuals who do not submit periodic CA paperwork.
5	B	6.3	6.2	6.7	R- 83	Increase/enforce penalties for not complying with CA reporting requirements.

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents (cont.)

5 B	5.8	5.9	5.1	R- 82	Provide rewards to personnel who are exceptionally conscientious in performing CA duties.
5 C	5.7	5.8	5.1	R- 79	Include CA as performance evaluation item for unit commanders, supervisors, all cleared personnel.
5 C	4.3	4.2	4.8	R- 80	Clarify the wording of the security item on the performance evaluation form.
5 D	5.8	6.0	5.0	R- 87	Develop better CA inspection checklists.
5 D	5.7	5.9	4.6	R- 89	Include CA in command inspections.
5 D	5.5	5.7	4.4	R- 90	Include CA on the IG.
5 D	4.7	4.8	3.8	R- 88	Increase the number and quality of CA inspections.
5 D	4.5	4.5	4.6	R- 73	Make CA records subject to frequent inspection and have violations result in criticism of the cmdr.
5 E	6.3	6.7	4.2	R-112	Develop better indicators for assessing the effectiveness of the CA program at each level.
5 E	5.6	5.8	4.7	R-113	Determine the effectiveness of different components of the CA program.
5 E	5.4	5.7	3.9	R-105	Develop weekly/monthly list of personnel security incidents & distribute list to unit security mgrs.
6 A	7.5	7.5	7.9	R- 12	Modify the regulations to direct other installation groups to provide more info to security office.
6 A	6.9	6.8	7.6	R- 13	Provide more guidance in regs on reporting reqmnts & implementation of CA procedures.
6 A	6.2	6.2	6.2	R- 14	Revise regs to increase the amount and types of derog. info that can be gathered by security office.
6 A	6.0	6.1	5.7	R- 15	Develop a standard security regulation or manual for unit security managers.
6 A	6.1	6.0	6.8	R- 8	Provide more detailed info in CA regulations.
6 A	5.6	5.7	5.6	R- 10	Organize CA regulations better (so it is easier to locate info).
6 A	5.1	4.8	6.6	R- 11	Modify CA regulations so that the text and examples are more consistent.
6 A	4.7	4.8	4.1	R- 9	Simplify CA regulations.
6 A	5.0	4.7	6.2	R- 24	Change regs to ensure police blotter info is given to the security office.
7 A	6.7	6.9	6.1	R-133	Take actions which encourage top levels...to make CA a higher priority.
7 A	3.5	3.6	3.0	R-132	Increase security office access to the installation commander.
7 B	5.2	5.4	4.3	R- 1	Increase funding for CA.
7 B	5.5	5.2	6.4	R- 5	Increase security office resources (computers, etc.).
7 B	3.4	3.7	2.2	R- 6	Redirect some resources from other security areas to CA.
7 B	2.7	2.7	2.6	R- 7	Redirect some resources from other areas of personnel security to CA.
7 C	6.7	6.9	6.0	R- 2	Increase number of personnel security office staff.
7 C	6.2	6.7	4.0	R- 96	Increase the number of security education personnel.
7 C	4.2	4.6	2.1	R- 4	Have a smaller number of unit sec mgrs who spend more time on CA.
7 C	3.3	3.3	3.3	R- 3	Increase number of unit security managers.
7 D	7.5	7.8	6.1	R-120	Create a separate, full-time position for personnel security officers.
7 D	5.1	5.4	3.7	R-118	Increase the grade level ceiling for senior security officers.
7 D	5.2	5.3	4.7	R-117	Increase the min. grade level of security officers.

Mean Ratings For 143 Recommendation Items for All Respondents, Collateral Site Respondents, and SCI Site Respondents (cont.)

7 D	5.1	5.3	4.2	R-119	Set a min. grade level for unit security managers.
8 A	6.3	6.5	5.4	R-129	Increase CA procedures directed at cleared federally employed civilians.
8 A	6.5	6.3	7.9	R- 93	Improve counseling/assistance for cleared individuals with security or suitability-related problems.
8 A	5.9	5.8	6.2	R- 22	Devote more CA effort to individuals who are at greatest security risk.
8 A	5.7	5.7	5.4	R-131	Devote more CA emphasis to individuals with TS level access.
8 B	6.8	6.9	6.3	R-138	Take steps to improve the "attitude toward personnel security" among installation personnel.
8 B	6.3	6.5	4.9	R-140	Consolidate the CA programs for all services into one single program.
8 C	6.2	6.2	5.7	R-127	Identify/clarify the legal concerns involved in the CA process and possible soi ions.
8 C	5.8	5.8	5.5	R-128	Change laws to reduce limitations & legal liability associated with reporting...personal behavior.
8 C	4.6	4.8	3.9	R- 60	Provide greater legal support for persons who report derog. info.
8 D	6.2	6.6	4.4	R-115	Reduce the number of persons requiring access to classified info.
8 D	6.1	6.5	4.5	R-114	Reduce the number of persons having security clearances.
8 D	5.7	6.0	4.4	R-116	Reduce the amt. of classified info produced.
8 E	4.4	5.1	2.8	R- 21	Conduct random investigations in addition to the required 5 year periodic reinvestigation.
8 E	4.7	4.7	4.7	R- 20	Gather systematic CA info on cleared ind'ls every 2 1/2 years after most recent redetermination.
8 E	3.1	3.3	2.6	R-139	Improve initial security clearance screening procedures.
8 F	6.1	6.1	5.6		
	----	----	----		
MEAN	5.47	5.56	5.03		
S.D.	1.14	1.12	1.56		

[1] See Table 6 for a listing of the taxonomy subcategories.

Note. Ratings were made on a "0" to "10" scale.

APPENDIX E:

Responses to 58 Open-ended Questions in Section 2 of the Security Officer Interview Protocol (Army, Air Force Navy Security Officers)

APPENDIX E

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS)

01. How could the local continuing assessment regulations be improved?

AR-AF-NV

10	8	10	Provide more detailed/specific information/guidance; have supplements
4	1	5	Keep regulations up-to-date; incorporate changes from other procedures
4	2	0	Reduce number of/integrate/simplify the regulations/supplements
1	1	1	Better index/structure the regulations
1	1	1	Improve command support
1	5	2	Other (e.g., automate; have better tracer actions; obtain more copies of regulations; assess security office performance; designate base department points of contact; require more communication with other departments; enforce regulations)

02. How could the (service branch) continuing assessment regulations be improved?

AR-AF-NV

11	14	12	Should be more detailed/specific/directive; eliminate contradictions
4	6	2	Make easier to read (better index/organize regulations; cross-reference material; use better paper/print)
4	6	1	Improve command support/involvement; specify base department responsibilities; coordinate regulations for security and other departments
2	2	3	Update regulations (there are too many messages/changes)
2	0	2	Simplify/reduce the number of regulations
4	3	4	Other (e.g., enforce regulations; provide more latitude for adjudication at the local level)

03. (For Collateral sites only) What changes should be made to the 5200.2-R (the governing directive covering minimum CA requirements for persons with collateral clearances)?

AR-AF-NV

10	0	1	Should be more detailed/specific/directive; eliminate contradictions
6	0	0	Make easier to read (better index/organize regulations; cross- reference material; use better paper/print)
1	2	0	Improve command support/involvement; specify base department responsibilities; coordinate regulations for security and other departments
3	0	0	Have DoD-wide regulations; have DoD-wide central adjudication agency
1	0	0	Simplify/reduce the number of regulations
4	0	1	Other

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

04. (For SCI sites only) What changes should be made to the DCID 1/14 (the governing directive covering CA requirements for persons with SCI access)?

AR-AF-NV

2	1	2	Should be more detailed/specific/directive
1	0	0	Improve command support/involvement
1	0	0	Have DoD-wide regulations
0	0	1	Have more updates
0	1	0	Increase use of polygraph counterintelligence questions
1	0	0	Other

05. Which two categories of derogatory information listed above account for most clearance revocations or discharges?

AR-AF-NV

11	11	10	Alcohol
10	13	8	Drugs
4	4	5	Financial
4	2	4	Emotional/mental/family
2	4	0	Criminal/felonies
0	3	0	Sexual misconduct
1	1	0	Falsification of information
0	1	0	Disloyalty to the U.S.
1	0	0	Foreign associations
2	1	2	Other incidents (e.g., NJPs, security violations, disciplinary incidents)

06. Which two types of derogatory information that are known to other persons or offices at the installation are least likely to be reported to the security office?

AR-AF-NV

9	11	7	Financial
9	10	8	Emotional/mental/family
6	7	9	Alcohol
4	2	3	Drugs
0	1	4	Sexual misconduct
1	1	0	Foreign associations
0	0	1	Falsification of information
0	1	0	Disloyalty to the U.S.
10	6	4	Other incidents (e.g., NJPs, disciplinary, security violations)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

07. Are there any other sources of derogatory information used at this installation that are not listed on pages 6 or 7 (of the interview protocol)?

AR	AF	NV	
16	17	16	no
1	0	1	yes - credit information
2	0	0	yes - periodic reinvestigations
0	0	2	yes - ex-spouses; citizens
0	1	0	yes - personal/pre-indoctrination interview
0	0	1	yes - inspections
0	0	1	yes - victims

08. What other formal or informal sources or methods of reporting derogatory information not listed above or currently used should be included as part of the continuing assessment program?

AR	AF	NV	
11	8	3	Credit/financial information (e.g. TRW, credit reports)
2	9	2	Computer databases (e.g., NCIC, OPM, INS, HQ)
0	4	5	Family members; friends; ex-spouses; citizens
6	9	12	Other (e.g., local mental health/social agencies; NACs; central adjudication agency information; civilian drug testing; store detectives; housing offices; polygraph; victims; base records)

09. For the two sources that you identified with the most unrealized potential usefulness, what could be done to make each source more useful?

AR	AF	NV	
6	8	7	Coworkers
7	3	7	Supervisors
4	5	6	Medical/employee assistance groups
2	4	3	Computer databases (e.g., NCIC, adjudication, headquarters)
3	2	3	Commanders
3	3	1	Personnel department
1	4	0	Credit information
2	1	1	Legal department
3	0	1	Local authorities
0	0	3	Headquarters; other commands
3	0	0	Investigations office; FBI
2	1	0	Polygraph
0	0	2	Informants
0	1	1	Subjects
0	2	3	Other (e.g., family members; drop boxes)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

10. Why are commanders sometimes reluctant to report derogatory information? (List the two most important reasons.)

AR-AF-NV

12	14	5	Operational readiness/mission concerns; loss of person; replacements are slow
7	7	5	Protect individual's career; person is friend
4	2	9	Perception that problem reflects commander's leadership; discredits unit; don't want to get involved
3	6	0	Information considered insignificant; lack of knowledge regarding reporting
3	2	1	Time commitment/paperwork
3	1	2	Commanders believe they can handle problem/distrust adjudication
2	1	2	Fear of reprisals/legal problems

11. Why are supervisors sometimes reluctant to report derogatory information? (List the two most important reasons.)

AR-AF-NV

11	14	7	Operational readiness/mission concerns; loss of person; replacements are slow
8	10	9	Protect individual's career; person is friend
2	2	9	Perception that problem reflects supervisor's leadership; discredits unit; don't want to get involved
7	1	5	Fear of reprisals/legal problems
1	7	3	Information considered insignificant; lack of knowledge regarding reporting
3	2	0	Time commitment/paperwork
1	1	0	Supervisors believe they can handle problem, distrust adjudication

12. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Subjects (i.e., self- reporting):

AR-AF-NV

9	4	9	Provide (partial) amnesty/assistance; reduce punishment for self-reporting; have a supportive command
7	9	5	Increase/improve security education/briefings; emphasize the importance of honesty
5	7	5	Have self-report form/interview/questionnaire
1	2	0	Increase/institute penalties for not self-reporting
2	1	0	Other

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

13. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Coworkers:

AR	AF	NV	
7	12	12	Increase/improve security education/awareness; emphasize responsibility for reporting
10	8	3	Provide anonymity/confidentiality/amnesty to those who report
3	3	1	Provide incentives/rewards for reporting
1	1	0	Create consequences for not reporting
2	0	0	Reduce punishment for those reported on
1	0	3	Other

14. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Supervisors:

AR	AF	NV	
10	14	14	Increase/improve security education/awareness; emphasize responsibility for reporting
3	2	3	Create consequences for not reporting; enforce reporting requirements
6	0	1	Include continuing assessment as a performance appraisal item; increase accountability
2	2	1	Provide anonymity/confidentiality/amnesty to those who report
4	1	0	Solve system problems (e.g., reduce adjudication time; have quick replacements)
0	4	1	Develop report form
0	1	0	Provide incentives/rewards for reporting
6	4	1	Other

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

15. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Unit commanders:

AR	AF	NV	
10	11	9	Increase/improve security education/awareness/briefings; emphasize responsibility for reporting
9	4	2	Include continuing assessment as a performance appraisal/IG item; increase accountability
1	6	0	Solve system problems (e.g., reduce adjudication time; have quick replacements)
3	2	1	Create consequences for not reporting; enforce reporting requirements
0	4	0	Develop report form/checklist; note derogatory information on existing forms
0	3	0	Include in unit commander regulations
4	5	1	Other

16. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Unit security managers:

AR	AF	NV	
7	7	2	Increase/improve security education/awareness
4	4	4	Increase/improve training (for unit security managers)
2	9	0	Make security a primary duty/full-time job; increase number of unit security managers
3	5	0	Provide unit security managers with more authority/access to information
1	1	0	Include continuing assessment as a performance appraisal item
2	0	0	Create consequences for not reporting
3	4	0	Other (e.g., have unit continuing assessment instructions; have anonymous reporting; develop better reporting forms)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

17. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Personnel department:

AR-AF-NV

6	7	9	Increase/improve security education/training; encourage them to report derogatory information
9	6	2	Incorporate continuing assessment into personnel department regulations; make reporting mandatory
3	5	1	Provide security office with access to additional information from personnel department (e.g., nonvoluntary discharges, PDs)
7	1	0	Improve/increase communication/contact with personnel department
4	3	3	Other (e.g., have memos of understanding between security office and personnel department; develop standard reporting form; automate reporting)

18. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Medical department:

AR-AF-NV

5	8	6	Increase/improve security education/training; encourage them to report derogatory information
9	8	0	Incorporate continuing assessment into medical department regulations; make reporting mandatory; increase regulation guidance
3	3	0	Gather more information on civilians (e.g., records; conduct drug tests; personality tests)
4	1	0	Improve/increase communication/contact with personnel department
2	3	2	Other (e.g., eliminate liability for reporting; have memos of understanding between security office and medical department; develop standard reporting form; have medical report derogatory information to commanders)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

19. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Legal department:

AR-AF-NV

9	7	0	Incorporate continuing assessment into legal department regulations; make reporting mandatory; increase regulation guidance
3	7	4	Increase/improve security education/training; encourage them to report derogatory information
7	2	0	Improve/increase communication/contact with legal department
0	2	1	Gather more information from legal department (e.g., court martials)
2	1	2	Other (e.g., eliminate liability for reporting; have memos of understanding between security office and legal department; develop standard reporting procedure; have legal department report derogatory information to commanders)

20. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Military police:

AR-AF-NV

4	3	6	Gather more information from military police (e.g., police blotter/reports); obtain derogatory information more quickly
1	7	2	Increase/improve security education/training; encourage them to report derogatory information
3	2	0	Improve/increase communication/contact with military police
3	1	0	Incorporate continuing assessment into military police regulations; make reporting mandatory; increase regulation guidance
5	2	2	Other (e.g., eliminate liability for reporting; have memos of understanding between security office and military police; assist base police in coordinating with local authorities; have incentives for reporting; obtain computers; obtain access to NCIC; develop standard reporting procedure)

21. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Other security offices on this installation:

AR-AF-NV

5	5	0	Improve/increase communication/contact with other security office(s)
2	5	0	Have security education on command mission; have common training; increase/improve training
4	0	0	Establish procedures for sharing derogatory information
0	1	0	Other (e.g., increase staff)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

22. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Other Installations:

AR-AF-NV			
7	8	8	Establish procedures for sharing derogatory information (e.g., have standard form/checklist)
3	2	1	Improve/increase communication/contact with other security office(s) (e.g., have annual meeting of security officers in local area)
0	2	2	Improve physical transfer of derogatory information (e.g., eliminate hand carrying; telefax information; automate)
4	0	0	Incorporate information sharing into regulations
0	3	1	Have security education; emphasize the need for sharing information
4	1	0	Other (e.g., have listing of all security officers in local region; enforce reporting requirements; use ASCAS code "Pending-A" code; retain records on microfiche)

23. [For each of the following groups, list two important changes that could be made to improve the reporting and quality of continuing assessment information being forwarded to the security office?] Investigations Office (e.g., CID, NIS, OSI)

AR-AF-NV			
6	8	3	Develop procedures for sharing derogatory information; establish agreement to share information; provide more timely information
7	2	1	Improve/increase communication/contact with investigations office
4	1	0	Incorporate information sharing into regulations; make reporting mandatory
1	2	0	Have security education; emphasize the need for sharing information
2	1	2	Other

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

24. How could the reporting and quality of continuing assessment information being forwarded on civilian personnel to the security office be improved?

AR-AF-NV

5	8	7	Increase/improve security education/training/awareness; encourage departments to report derogatory infonnation; clarify legal issues in reporting
4	4	4	Gather more information from departments, local authorities, derogatory information sources; reduce "red tape" for obtaining information
6	2	0	Incorporate continuing assessment into department regulations; make reporting mandatory; correct conflicting regulations
0	5	0	Use computer databases (e.g., NCIC)
2	2	0	Make civilian and military security program more similar
1	1	2	Improve/increase communication/contact with departments
1	1	1	Develop standard forms for reporting/gathering derogatory information
4	7	1	Other (e.g., be proactive in gathering derogatory information; have penalties for non-compliance with security responsibilities; have departments submit recommendation on retaining access; devote more resources to continuing assessment; ensure clearance eligibility prior to hire)

25. How could the reporting and quality of continuing assessment information being forwarded on military personnel to the security office be improved?

AR-AF-NV

5	8	13	Increase/improve security education/training/awareness; encourage departments to report derogatory infonnation
6	5	3	Gather more information from departments, local authorities, derogatory information sources; reduce "red tape" for obtaining information
2	3	1	Develop standard forms for reporting/gathering/retaining derogatory information
4	1	1	Incorporate continuing assessment into department regulations; make reporting mandatory; correct conflicting regulations
1	1	3	Improve/increase communication/contact with departments
1	1	2	Use/develop computer databases (e.g., NCIC)
2	0	0	Have consequences for non-compliance; enforce requirements
2	5	0	Other (e.g., have proactive procedures; increase resources devoted to personnel security; provide anonymity to those who report

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

26. Do some units do a much better job than others of reporting valid derogatory information to the security office? (If yes, what might account for this?)

AR-AF-NV	
4 0 2	no
11 12 8	yes - education, training, experience, and knowledge of unit personnel
10 12 3	yes - interest, commitment, and support of unit personnel
0 7 2	yes - unit mission and amount of classified information
2 5 1	yes - resources devoted to security (e.g., number of security personnel; full- time security managers)
1 2 1	yes - amount of security education
2 0 1	yes - relationship with security office
5 2 2	yes - other (e.g., organization size; morale; using structured forms)

27. What critical information relevant to continuing assessment does the security office need but not have access to and who currently retains this information? This could be information held other groups at the installation, by central recordkeeping facilities, or by other commands.

AR-AF-NV	
15 8 5	Criminal information; police/blotter; disciplinary actions; legal information
5 17 8	Medical/social actions/mental health
11 4 2	Financial (e.g., credit information, collection agency letters)
10 2 3	Drug/alcohol
5 3 2	Personnel records; performance information
7 7 6	Other (e.g., Unfavorable Information Files; PIFs; DCII; 398s; investigation records)

28. What critical information which is typically purged at different times (e.g., during transfers, reenlistments) should be kept to enable better continuing assessment of personnel?

AR-AF-NV	
16 7 4	Article 15s, NJPs, letters of reprimand, 110s
5 1 1	Local police records/blotter information; investigations
7 5 6	Unspecified derogatory information; PIFs
5 2 2	Employee assistance records (e.g., drug, alcohol, medical)
4 2 0	Letters of clearance suspension/revocation
1 1 2	Financial (e.g., credit information, collection agency letters)
1 6 3	Other

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

29. How could the transfer of continuing assessment information from one command to another be improved?

AR-AF-NV

AR	AF	NV	
9	2	3	Create a checklist/form; develop a security file
7	5	1	Eliminate hand carrying of records; use telefax to transfer records; send records via express or registered mail; seal records
4	2	2	Include more derogatory information; have more timely submissions
1	3	2	Use automated channels and centralized computer database; use microfiche
7	7	9	Other (e.g., administer a self-report form at time of transfer; forward documents between security officers; have designated person at each site to receive documents; have penalties for non-compliance; modify regulations on this; include this as an inspection item; improve transfer of records between different military services; inform gaining unit of derogatory information)

30. How could continuing assessment recordkeeping procedures be improved?

AR-AF-NV

AR	AF	NV	
7	11	4	Automate recordkeeping; improve software
5	1	1	Standardize recordkeeping procedures/requirements/forms; have recordkeeping checklist
3	3	0	Increase resources (e.g., manpower, equipment, computers, class A phones)
3	0	1	Develop new reports (e.g., monthly unit security manager report, 380- 12 report)
2	0	1	Develop security files/folders; keep better files
2	0	1	Create a recordkeeping system
2	5	4	Other (e.g., get quarterly status report from central adjudication agency; input own tracers; improve coordination; have better guidelines on what can/cannot be purged; centralize installation records)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

31. What actions could be taken to increase the involvement and support of the installation commander in the continuing assessment process?

AR-AF-NV

8	9	5	Make personnel security a performance appraisal/inspection item; increase commander's accountability; have annual certification by commander that program has been reviewed
7	12	0	Keep commander more informed on security through meetings/updates/status reports
3	4	6	Increase education; have security course for commander
3	0	1	Have commander increase resources for continuing assessment program
0	2	0	Modify regulations to emphasize personnel security
2	0	0	Have commander sign letter supporting the program
3	1	0	Other (e.g., develop better recordkeeping procedures; increase emphasis from higher commands)

32. What actions could be taken to increase the involvement and support of unit commanders in the continuing assessment process?

AR-AF-NV

8	6	3	Increase education/training; have security course for unit commanders
5	4	2	Make personnel security a performance appraisal/inspection item; increase commander's accountability
8	3	0	Make reporting of derogatory information a requirement; enforce regulations; establish/improve procedures for reporting derogatory information
0	5	2	Keep commander more informed on security through meetings/updates/status reports
6	5	3	Other (e.g., have penalties for noncompliance with security regulations; require unit commanders to administer security education; have unit commanders work more closely with security office/respond more quickly to security matters; increase emphasis on security from higher command; have better liaison with unit commanders; provide commendations for good performance; have commander sign a letter supporting the security program)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

33. What could be done to improve the use of incentives as a tool for improving continuing assessment?

AR-AF-NV

7	0	8	Should not use incentives
5	13	8	Use incentives (e.g., monetary awards, commendations, medals, recognition, letters of appreciation, plaques, certificates of accomplishment, notices in the paper, notice in personnel file)
2	4	2	Other (e.g., ensure anonymity/amnesty for sources; make security a performance appraisal item; emphasize the positive aspects of continuing assessment)

34. What indicators, if any, are used by inspectors to evaluate the effectiveness of the continuing evaluation program?

AR-AF-NV

3	1	7	None
9	5	3	Examine records for currency, accuracy, organization (e.g. compare roster of cleared persons having derogatory information with personnel file; compare headquarters files with command files; ensure appropriate reports are being made)
3	10	0	Number and types of SSFs/PDRs/SAERs/security violations/Article 15s; established suspense system; number on suspension list
3	6	1	Periodic reinvestigations (timeliness)
4	3	1	Sensitivity of positions to which people are assigned; ASCAS roster
2	3	3	Knowledge of persons being inspected; knowledge of reportable derogatory inforamtion by supervisors, commanders, security managers
3	1	3	Inspection checklist/results; self-inspection results
2	0	2	SBI/BI packets; NAC dates
2	0	0	Interim security clearances/clearance waivers
2	0	0	Time taken for final adjudication/submission of information to central adjudication agency
3	8	2	Other (e.g , number in drug rehabilitation; security awareness training; check briefings; tracers sent out; program reviews; number in pending adjudication)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

35. What could be done to improve the inspection process as a tool for improving continuing assessment?

AR-AF-NV

3	5	4	Have standard inspection checklist/criteria
3	3	2	Have inspections; increase frequency/thoroughness of inspections
5	1	1	Devote more resources (personnel, time) to inspections
1	5	1	Interview supervisors, unit commanders, cleared individuals
2	0	2	Have full-time/better trained inspectors
3	0	0	Have mandatory inspections
3	0	0	Have follow-up/compliance inspections
2	0	0	Customize inspections to local unit
10	12	7	Other (e.g., inspect training programs; increase command emphasis on inspections; compare personnel and security records; check number of cleared personnel; increase inspection statistics; test knowledge of security officers; have inspectors provide more training/feedback; spot check records; include as special interest item on IG)

36. Given current resources, do you think personnel without security clearances should be included in the continuing assessment program? (If yes/no, why?)

AR-AF-NV

7	3	4	yes - they might obtain access later
3	2	2	yes - it is their responsibility also; they should be security conscious
1	3	3	yes - they could be exposed to/around classified information
0	1	0	yes - they also possess important information
0	1	3	yes
6	3	1	yes - insufficient resources; too much paperwork/time/money

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTI0N 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

37. Is more continuing assessment effort directed to persons with Top Secret clearances (as opposed to persons with Secret clearances at this installation)? (If yes, how do continuing assessment procedures differ for these groups?)

AR	AF	NV	
9	7	11	no
6	3	2	yes - Top Secret undergo periodic reinvestigations
1	2	1	yes - Top Secret receive more attention
0	2	0	yes - Top Secret receive better information, more briefings/training
2	0	2	yes

38. Given current resources, how much emphasis in the continuing assessment should be given to individuals with Secret-level access as opposed to persons with Top Secret-level access?

AR	AF	NV	
10	5	8	same
6	8	7	more emphasis for Top Secret
1	1	0	more emphasis for both groups
0	2	0	more emphasis for Secret (so both groups have a more similar amount of emphasis)

39. Is more continuing assessment effort directed to particular positions at this installation (excluding PRP billets)? (If yes, which types of positions receive more attention from a continuing assessment standpoint?)

AR	AF	NV	
11	9	10	no
7	8	7	yes - Top Secret/SCI personnel; SAP/presidential support/SIOP personnel

40. Is more continuing assessment effort directed to particular positions at this installation (excluding PRP billets)? (If yes, how do continuing assessment procedures differ for these groups?

AR	AF	NV	
11	9	10	no
1	5	5	yes - more command emphasis; more careful supervision
2	0	1	yes - more/more thorough briefings
0	1	1	yes - other (e.g., medical records are flagged; random polygraphs)
4	2	0	yes - (no specific information given)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTI0N 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

41. Are there differences in continuing assessment procedures for military and civilian personnel at this installation? (If yes, what are the biggest differences?)

AR	AF	NV	
12	11	11	no
3	7	1	yes - more difficult to obtain information on/take action on civilians
1	3	1	yes - random drug testing for military personnel but not for civilians
5	1	1	yes - other

42. Are there any challenges or problems associated with this continuing assessment program that are unique or more frequent because this installation is located in the continental U.S. as compared to overseas? (If yes, what are these unique or more frequent problems?)

AR	AF	NV	
9	10	9	no
10	9	9	yes

yes - in CONUS (less control over individuals; more privacy act protections; continuing assessment may get less emphasis; high drug problem in some areas; work group less close-knit than overseas)

yes - in OCONUS (closer proximity to designated countries; more travel to designated countries; foreign laws create additional problems for the security office; large naturalized populations at bases; culture differences; more difficulty communicating with adjudication agency; more marriages to local nationals; high cost of living)

43. Should more continuing assessment emphasis be directed to installations located in certain geographic areas (e.g., overseas, in high cost areas, near Soviet consulate)? (If yes, which geographic areas should receive more attention from a continuing assessment standpoint?)

AR	AF	NV	
2	3	1	no
7	8	2	yes - overseas
3	4	4	yes - near/in designated countries/consulates
10	1	0	yes - Europe (especially Germany)
6	2	0	yes - Far East (especially Korea)
0	3	1	yes - Baltic/Mediterranean countries
2	0	0	yes - Panama
2	0	0	yes - Middle East
4	1	2	yes - California (especially near San Francisco)
3	0	4	yes - Washington D.C./Norfolk
0	4	5	yes - high threat areas
2	2	0	yes - high cost areas
3	5	3	yes - other (e.g., emphasize different aspects of the program depending on the specific risks of the location; isolated ports, other selected U.S. cities.)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

44. What statistics relevant to continuing assessment are kept by the security office?

AR-AF-NV

7	3	10	None
13	1	0	Number and types of clearances
4	8	3	Number of clearance suspensions/revocations; SSFs; SAERs
0	4	0	Status of periodic reinvestigations
9	13	3	Other (e.g., number of violations; inspection results; foreign travel records; amount of classified information; reports to commander; security education/briefing records)

45. What indicators does the security office use to evaluate the effectiveness of continuing assessment?

AR-AF-NV

2	1	9	None
11	14	5	Number of security violations; number/amount of reported derogatory incidents/incident reports; UIFs; clearance suspensions/revocations
5	7	1	Inspection results; office assistance visit results; self-inspections; program reviews
3	2	2	Feedback/calls from security managers/commanders; quarterly meetings
4	1	0	Periodic reinvestigations (timeliness)
10	11	2	Other (e.g., knowledge of supervisors and coworkers; number of 398s returned from central adjudication agency; results of training exercises; security education/training participation/courses)

46. What indicators does the installation commander use to monitor the effectiveness of the continuing assessment program?

AR-AF-NV

7	3	9	None
2	2	5	Number of security violations; clearance suspensions/revocations
5	4	0	Inspection results; office visits; program reviews
1	6	2	Contact with security office; meetings; reports from security office
2	0	1	Lack of complaints about security
1	1	0	Number and types of clearances
3	4	3	Other (e.g., training records; currency of investigations knowledge of supervisors and coworkers; results of training exercises)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTI0N 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

47. What information relevant to continuing assessment do these employee assistance programs have that the security office needs but does not have access to and who has this information?

AR	AF	NV	
9	7	8	Medical/emotional/mental/family
11	7	4	Alcohol/drugs
12	7	3	Financial
3	6	2	Criminal/felonies/legal
4	3	1	Sexual misconduct
0	3	0	Other

48. How could we encourage employee assistance personnel to share information relevant to continuing assessment with the security office?

AR	AF	NV	
6	10	8	Increase security education/awareness; include this in their training
11	9	2	Include continuing assessment in their regulations; make reporting mandatory; resolve conflicting regulations
2	2	4	Have employee assistance groups provide additional information; provide more timely information; implement existing procedures
0	4	1	Have standard/PRP-type reporting form/checklist
1	1	0	Establish memos of understanding
10	2	0	Other (e.g., change laws; share information through personnel department; make individuals sign employee assistance records release as a job requirement; increase communication with employee assistance)

49. What could be done to improve security counseling as it relates to continuing assessment?

AR	AF	NV	
3	9	8	Educate/train persons who provide counseling
8	4	5	Increase security education; advertise that program exists
3	5	2	Initiate a program
5	1	2	Increase resources (e.g., personnel; time) for counseling
0	0	2	Increase security counseling
1	3	1	Other (e.g., put this into unit security managers' regulations; have security office staff/high level personnel provide counseling; make counseling mandatory for those who have derogatory information)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

50. What could be done to improve the effectiveness of training for security staff with respect to continuing assessment?

AR	AF	NV	
12	9	13	Have training/more training/ongoing training/service/command-sponsored seminars
2	16	2	Have better/standardized/up-to-date training procedures/guides/ materials
8	1	0	Increase resources for training
3	0	2	Use/develop correspondence course
3	0	0	Have mobile training teams
10	5	2	Other (e.g., establish policies/procedures; have interview skills training; develop service specific courses; have field trips to DIS/CCF; enforce security regulations; make training more interesting; have intelligence personnel administer training; certify training personnel; make persons accountable for attending training)

51. What could be done to improve security education procedures with regard to the continuing assessment program?

AR	AF	NV	
8	3	5	Have more/better publications/pamphlets/newsletter/training materials/posters; develop handbook
7	2	5	Increase/emphasize security education
2	4	4	Have more/better videos
8	0	2	Increase resources (time; personnel; money)
0	3	6	Provide guidance on content/indicators
0	3	3	Have others provide training (e.g., supervisors, unit commanders, DIS or agency representative; persons who committed violations; department point of contacts)
1	2	0	Standardize security education procedures
1	1	1	Have better regulatory guidance
1	1	0	Include security in supervisor/commander/department training classes, during in-processing
1	0	0	Train security staff
7	6	6	Other (e.g., develop computerized individual risk assessment; develop a listing of POCs and their phone numbers; institute penalties for non-compliance with security procedures; test those who handle classified information; increase command involvement/support; document security education: make security education mandatory)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

52. What can be done to improve the effectiveness of security briefings with respect to continuing assessment?

AR	AF	NV	
6	6	3	Increase frequency of/time devoted to/emphasis on/standardization of briefings
6	2	4	Have more innovaiive/interesting briefings (e.g., cite actual spy cases
5	4	1	Have more/better/standardized handouts/briefing materials
5	2	3	Increase resources (time; personnel; money)
3	2	1	Have more/better/standardized videos
1	2	3	Provide guidance on indicators/content
3	0	1	Increase command emphasis on briefings
1	0	2	Have others provide briefings (e.g., persons who committed violations; commanders; supervisors)
4	6	2	Other (e.g., make attendance mandatory; have briefing checklist; train security staff)

53. In summary, what aspects of the continuing assessment program at this installation are working best?

AR-	AF-	NV	
3	6	10	Reporting/cooperation from installation departments (e.g., military police, personnel office, employee assistance, investigations office)
5	6	1	Reporting/cooperation from coworkers/supervisor/commanders/unit security managers
1	0	0	Reporting/cooperation from local authorities, other commands
4	4	2	Reporting of derogatory information; reporting procedures
7	6	4	Security education/awareness/counseling
6	2	7	Security briefings
9	2	7	Coordination with adjudication agency/headquarters; clearance suspension/revocation process; quick actions taken when derogatory information is found
8	6	0	Periodic reinvestigations
1	3	2	Local/service regulations/supplements
1	4	1	Dedicated/experienced/full-time security staff
1	2	1	Security office/unit security manager training
0	1	2	Command emphasis/support
1	2	0	Inspections
5	4	5	Other (e.g., controlling numbers with access; reports)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN
SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL
(ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

54. In summary, what aspects of the continuing assessment program at this installation are not working?

AR-AF-NV

8	7	6	Lack of reporting/cooperation from installation departments (e.g., personnel office, employee assistance)
4	9	0	Lack of reporting/cooperation from coworkers, supervisor, commanders
2	1	1	Lack of reporting/cooperation from local authorities, other commands
2	1	0	Lack of self-reporting
6	7	5	Security education/awareness/counseling
7	3	0	Difficulties with adjudication agency/headquarters
3	3	4	Reporting of derogatory information; reporting procedures
3	3	1	Lack of command emphasis
2	0	6	Lack of security staff training
2	1	3	Performance appraisals
2	0	3	Regulations
0	1	4	Recordkeeping procedures
2	1	3	No incentives for reporting derogatory information
0	3	1	Lack of resources (e.g., personnel, time)
0	1	3	Inspections; continuing assessment is not included in the IG
6	8	5	Other (e.g., no consequences for non-compliance with security regulations/responsibilities; poor indicators of security risk; little derogatory information gathered on civilians; poor indicators of program effectiveness)

55. In your opinion, what is the single most important factor in developing an effective continuing assessment program?

AR-AF-NV

10	12	6	Security education/awareness/training
6	1	3	Resources; good security personnel
2	3	4	Cooperation from derogatory information reporting sources
2	2	4	Good regulations; enforce regulations
1	4	1	Other (e.g., reduce number of persons with clearances; target continuing assessment efforts towards certain groups; communication and feedback among personnel involved in the personnel; top management support; information flow and feedback from central adjudication agency)

RESPONSES TO 58 OPEN-ENDED QUESTIONS IN SECTION 2 OF THE SECURITY OFFICER INTERVIEW PROTOCOL (ARMY, AIR FORCE NAVY SECURITY OFFICERS cont.)

56. Overall, to what extent is significant derogatory information reaching unit commanders?

AR-AF-NV

0	1	0	100 percent of information received/known
0	0	1	100 percent
1	4	0	90 to 99 percent
4	5	3	70 to 89 percent; very good; well
4	2	7	50 to 69 percent; adequately; good; most
0	3	0	25 to 49 percent
5	2	0	Less than 25 percent; infrequently; very little

57. Overall, to what extent is significant derogatory information being reported to the adjudication agency?

AR-AF-NV

9	8	6	100 percent of information received/known
1	0	1	90 percent of information received/known
1	0	0	Everything of value
2	1	0	100 percent
1	0	0	90 to 99 percent
0	4	4	70 to 89 percent
2	3	1	50 to 69 percent
0	1	0	25 to 49 percent
1	1	0	Less than 25 percent

58. Overall, which type of continuing assessment program is better, one which reports only significant derogatory information to adjudication and suspends an individual's access or one which reports all derogatory information to adjudication and may or may not suspend an individual's access? Why?

AR-AF-NV

10	6	8	All - need complete picture/whole person concept; assess historical trends
2	1	0	All - let adjudication agency determine what is significant; reporting only significant information would discourage reporting
1	3	1	All - required by regulations; need detailed guidance
2	2	2	Significant - a lot of the information is not relevant; adjudication agency overreacts/handle additional information poorly
1	4	1	Significant - inefficient to report all derogatory information
1	3	0	Significant - minor things would slow system down more
1	2	2	Significant

APPENDIX F:

Quantitative Interview Protocol Results for Service Branch Groups

Adequacy of continuing assessment regulations
(1="Highly inadequate" and 10="Excellent")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Locally-developed CA regulations	MEAN	6.0	6.2	6.2	7.5	7.8	7.7	8.0	4.6	5.2	7.1	6.3	6.4
	N	3	14	17	4	12	16	2	11	13	9	37	46
Service branch CA regulations	MEAN	5.0	6.3	6.1	7.0	6.5	6.7	6.5	6.7	6.7	6.3	6.5	6.5
	N	3	15	18	5	15	20	4	14	18	12	44	56
5200.2-R (for collateral clearances)	MEAN	5.0	6.5	6.4	.	7.2	7.2	.	6.0	6.0	5.0	6.6	6.5
	N	1	14	15	0	4	4	0	3	3	1	21	22
DCID 1/14 (for SCI access)	MEAN	6.3	7.0	6.5	7.0	.	7.0	7.0	.	7.0	6.7	7.0	6.8
	N	3	1	4	2	0	2	3	0	3	8	1	9

Number of Valid Derogatory Incidents in Each Category

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Alcohol abuse incidents	MEAN	17.0	32.8	30.2	47.8	101.3	87.2	9.3	36.3	30.3	27.3	56.2	49.9
	N	3	15	18	5	14	19	4	14	18	12	43	55
Drug abuse incidents	MEAN	8.7	41.3	35.9	12.2	33.3	27.7	6.7	17.1	14.8	9.5	30.8	26.2
	N	3	15	18	5	14	19	4	14	18	12	43	55
Financial problems	MEAN	9.7	13.5	12.9	24.4	15.2	17.6	9.3	14.2	13.1	15.7	14.3	14.6
	N	3	15	18	5	14	19	4	14	18	12	43	55
Emotional/ mental/family problems	MEAN	6.0	11.3	10.4	12.6	12.5	12.5	4.7	11.5	10.0	8.3	11.7	11.0
	N	3	15	18	5	14	19	4	14	18	12	43	55
Criminal felony acts	MEAN	5.3	7.5	7.2	3.4	36.1	27.5	1.0	4.2	3.5	3.1	15.7	13.0
	N	3	15	18	5	14	19	4	14	18	12	43	55
Sexual misconduct incidents	MEAN	0.7	5.0	4.3	8.6	14.6	13.1	1.0	2.2	1.9	4.1	7.2	6.5
	N	3	15	18	5	14	19	4	14	18	12	43	55
Disloyalty to the U.S. incidents	MEAN	0.3	0.1	0.1	0.8	0.6	0.7	0.2	0.3	0.3	0.5	0.3	0.4
	N	3	15	18	5	14	19	4	14	18	12	43	55
Foreign association/travel incidents	MEAN	1.7	1.0	1.1	7.4	0.4	2.3	2.5	0.2	0.7	4.3	0.5	1.4
	N	3	15	18	5	13	18	4	14	18	12	42	54
Falsification of information acts	MEAN	0.7	30.3	25.4	2.0	3.9	3.4	1.0	1.9	1.7	1.3	12.5	10.0
	N	3	15	18	5	14	19	4	14	18	12	43	55
Security violation incidents	MEAN	22.7	5.8	8.6	27.6	13.6	17.3	8.5	9.8	9.5	20.0	9.6	11.9
	N	3	15	18	5	14	19	4	14	18	12	43	55
Court martials/ desertions	MEAN	0.0	3.0	2.5	3.2	39.0	29.6	0.0	1.8	1.4	1.3	14.6	11.7
	N	3	15	18	5	14	19	4	13	17	12	42	54
Other incidents	MEAN	9.0	32.9	28.9	58.0	68.6	65.8	6.5	30.9	25.2	28.6	44.2	40.7
	N	3	15	18	5	14	19	4	13	17	12	42	54

Percentage of valid derogatory incidents in the past 12 months

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Involving military personnel	MEAN	48.3	57.5	56.1	83.7	79.3	80.2	97.2	71.7	78.1	79.0	69.0	71.1
	N	3	16	19	4	15	19	4	12	16	11	43	54
Involving civilian personnel	MEAN	51.7	36.2	38.7	17.5	20.7	20.1	2.7	36.7	28.2	21.5	31.0	29.0
	N	3	16	19	4	15	19	4	12	16	11	43	54

Percentage of reported derogatory information that is actually valid

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Valid percentage	MEAN	90.0	87.2	87.6	96.3	88.8	90.5	90.0	94.2	93.2	91.9	89.8	90.3
	N	3	16	19	3	10	13	4	12	16	10	38	48

Usefulness of Sources of Derogatory Information
(1="Very little usefulness" and 10="Extremely useful")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Subject (self-reports)	MEAN	4.7	8.3	7.2	8.5	5.7	6.8	8.0	5.0	6.0	6.9	6.6	6.7
	N	3	7	10	2	3	5	3	6	9	8	16	24
Coworkers	MEAN	9.0	5.6	5.9	7.0	6.2	6.4	4.3	5.6	5.1	5.8	5.7	5.7
	N	1	10	11	1	4	5	3	5	8	5	19	24
Supervisors	MEAN	8.3	7.4	7.6	8.5	6.8	7.1	7.2	7.1	7.1	7.9	7.1	7.3
	N	3	11	14	2	9	11	4	12	16	9	32	41
First sergeant /Leading PO /Chief	MEAN	7.0	8.4	8.3	7.3	7.4	7.4	7.0	6.5	6.7	7.1	7.5	7.4
	N	1	7	8	3	10	13	4	6	10	8	23	31
Unit commanders	MEAN	8.5	8.1	8.1	8.0	7.9	7.9	7.5	7.0	7.2	7.9	7.8	7.8
	N	2	13	15	4	14	18	4	5	9	10	32	42
Installation commander	MEAN	10.0	8.0	8.4	.	4.3	4.3	5.0	8.4	8.0	7.5	7.4	7.4
	N	1	4	5	0	3	3	1	7	8	2	14	16
Unit security managers	MEAN	8.5	7.5	7.7	6.0	7.5	7.4	8.0	4.5	5.7	7.7	7.3	7.4
	N	2	11	13	1	13	14	1	2	3	4	26	30
Investigations office	MEAN	9.0	6.7	6.9	9.0	8.9	8.9	6.0	8.8	8.3	7.8	8.1	8.1
	N	1	12	13	2	14	16	2	9	11	5	35	40
Federal agencies	MEAN	10.0	8.0	8.5	8.0	5.7	6.2	.	9.0	9.0	9.3	7.5	7.9
	N	2	6	8	1	4	5	0	3	3	3	13	16
Personnel department	MEAN	.	6.5	6.5	3.0	7.0	6.3	.	8.8	8.8	3.0	7.2	6.9
	N	0	8	8	1	5	6	0	4	4	1	17	18
Medical department	MEAN	8.0	7.1	7.2	3.0	7.4	6.7	8.0	9.0	8.9	6.3	7.7	7.6
	N	1	9	10	1	5	6	1	6	7	3	20	23
EAP groups/ social actions	MEAN	.	6.0	6.0	7.0	7.0	7.0	7.5	8.2	8.0	7.2	7.4	7.4
	N	0	2	2	2	3	5	2	5	7	4	10	14
Legal department	MEAN		8.4	8.4	7.0	7.0	7.0	10.0	7.5	7.9	8.5	7.7	7.8
	N	0	7	7	1	6	7	1	6	7	2	19	21
Other security office(s)	MEAN	8.5	8.2	8.3	4.0	7.6	7.2	4.5	8.0	6.6	6.0	8.0	7.6
	N	2	9	11	1	8	9	2	3	5	5	20	25
Military police	MEAN	5.0	9.0	8.6	6.5	8.6	8.4	3.5	8.4	7.4	5.0	8.7	8.2
	N	1	9	10	2	15	17	2	8	10	5	32	37

(CONTINUED)

Usefulness of Sources of Derogatory Information
(1="Very little usefulness" and 10="Extremely useful")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Police blotter	MEAN	10.0	8.6	8.7	8.0	9.1	8.9	3.5	8.7	7.4	6.6	8.8	8.5
	N	1	12	13	2	15	17	2	6	8	5	33	38
Local civilian police	MEAN	.	7.1	7.1	.	6.8	6.8	5.5	7.1	6.8	5.5	7.0	6.9
	N	0	7	7	0	6	6	2	8	10	2	21	23
Other local authorities	MEAN	.	10.0	10.0	.	4.7	4.7	.	5.6	5.6	.	6.2	6.2
	N	0	2	2	0	3	3	0	5	5	0	10	10
Local newspapers	MEAN	8.5	6.2	6.7	3.0	4.7	4.6	2.0	3.5	3.0	4.8	5.1	5.0
	N	2	8	10	1	8	9	2	4	6	5	20	25
Law enforcement databases	MEAN	6.0	7.2	7.0	.	6.6	6.6	.	7.0	7.0	6.0	6.9	6.9
	N	1	5	6	0	5	5	0	4	4	1	14	15
Other computer databases	MEAN	.	.	.	.	8.0	8.0	.	.	.	.	8.0	8.0
	N	0	0	0	0	1	1	0	0	0	0	1	1
Hotline information	MEAN	.	3.0	3.0	.	8.0	8.0	1.0	3.0	2.5	1.0	3.8	3.4
	N	0	2	2	0	1	1	1	3	4	1	6	7
Random drug testing	MEAN	1.0	6.5	6.1	.	9.8	9.8	7.5	9.5	9.1	5.3	8.0	7.7
	N	1	13	14	0	4	4	2	8	10	3	25	28
"Silent listening posts"	MEAN	.	5.5	5.5	.	5.5	5.5	1.3	4.7	3.0	1.3	5.1	4.0
	N	0	2	2	0	2	2	3	3	6	3	7	10
Other installations/ commands	MEAN	5.0	7.6	6.8	6.5	5.8	5.9	7.5	7.1	7.2	6.1	6.7	6.6
	N	3	7	10	2	9	11	2	8	10	7	24	31
Central adjudication facility	MEAN	5.7	8.5	7.9	7.7	8.2	8.1	5.5	7.9	7.5	6.4	8.2	7.9
	N	3	13	16	3	14	17	2	9	11	8	36	44
Drop boxes	MEAN	.	.	.	.	.	.	1.0	10.0	4.0	1.0	10.0	4.0
	N	0	0	0	0	0	0	2	1	3	2	1	3
Post Cards	MEAN	.	1.0	1.0	.	.	.	.	3.0	3.0	.	1.7	1.7
	N	0	2	2	0	0	0	0	1	1	0	3	3
Chaplain	MEAN	.	.	.	.	.	.	.	10.0	10.0	.	10.0	10.0
	N	0	0	0	0	0	0	0	1	1	0	1	1
Neighbors	MEAN	2.0	5.7	5.0	.	3.0	3.0	2.0	4.0	3.0	2.0	5.0	4.2
	N	1	4	5	0	1	1	1	1	2	2	6	8

Willingness of Different Groups to Share Relevant Information
(1="Very unwilling" and 10="Very willing")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Subject	MEAN	3.7	2.6	2.8	1.7	2.1	2.1	4.0	2.1	2.5	3.2	2.3	2.5
	N	3	14	17	3	14	17	4	13	17	10	41	51
Coworkers	MEAN	3.0	3.8	3.6	2.3	2.6	2.6	4.0	3.2	3.4	3.2	3.2	3.2
	N	3	14	17	3	14	17	4	13	17	10	41	51
Supervisors	MEAN	5.0	5.7	5.6	2.3	5.5	5.0	5.7	6.4	6.2	4.5	5.8	5.6
	N	3	15	18	3	15	18	4	13	17	10	43	53
First sergeant /Leading PO /Chief	MEAN	3.5	6.4	6.0	4.7	6.9	6.5	6.7	7.1	7.0	5.3	6.8	6.5
	N	2	12	14	3	15	18	4	10	14	9	37	46
Unit commanders	MEAN	6.3	7.6	7.4	3.3	6.9	6.3	8.7	6.6	7.2	6.1	7.1	6.9
	N	3	14	17	3	15	18	3	8	11	9	37	46
Installation commander	MEAN	7.0	6.1	6.2	5.5	7.9	7.4	8.7	8.6	8.6	7.2	7.3	7.3
	N	3	14	17	2	8	10	3	10	13	8	32	40
Unit security managers	MEAN	6.0	7.3	7.1	6.3	7.5	7.3	10.0	6.5	7.0	6.8	7.3	7.2
	N	2	13	15	3	15	18	1	6	7	6	34	40
Investigations office	MEAN	3.3	7.0	6.4	6.7	8.0	7.8	5.2	8.8	7.9	5.1	7.9	7.4
	N	3	14	17	3	15	18	4	12	16	10	41	51
Federal agencies	MEAN	3.7	7.9	7.1	5.0	3.0	3.4	3.0	6.0	5.3	3.7	5.9	5.4
	N	3	12	15	2	9	11	3	10	13	8	31	39
Personnel department	MEAN	1.3	5.1	4.4	6.5	5.6	5.7	5.3	6.0	5.9	4.1	5.5	5.3
	N	3	15	18	2	12	14	3	13	16	8	40	48
Medical department	MEAN	5.3	6.1	6.0	1.7	4.9	4.3	4.7	6.0	5.7	4.0	5.7	5.3
	N	3	14	17	3	14	17	4	13	17	10	41	51
Employee assistance groups	MEAN	1.5	2.8	2.6	1.0	4.4	3.7	7.2	4.6	5.2	3.9	3.9	3.9
	N	2	13	15	3	13	16	4	12	16	9	38	47
Legal department	MEAN	2.5	5.4	5.0	3.0	7.2	6.9	5.0	7.0	6.5	4.0	6.5	6.1
	N	2	14	16	1	15	16	4	12	16	7	41	48
Other security offices	MEAN	6.5	8.8	8.4	4.7	8.5	7.7	6.0	7.2	7.1	5.5	8.3	7.8
	N	2	12	14	3	11	14	1	8	9	6	31	37
Military police	MEAN	4.5	8.9	8.3	8.7	9.5	9.3	6.5	7.3	7.1	6.8	8.7	8.3
	N	2	12	14	3	15	18	4	10	14	9	37	46

(CONTINUED)

Willingness of Different Groups to Share Relevant Information
(1="Very unwilling" and 10="Very willing")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Local civilian police	MEAN	3.3	5.2	4.8	5.5	6.6	6.4	6.0	6.5	6.4	4.7	6.0	5.8
	N	3	13	16	2	12	14	2	11	13	7	36	43
Other local authorities	MEAN	2.3	4.5	4.1	5.5	4.6	4.7	3.5	6.3	5.8	3.6	5.1	4.8
	N	3	12	15	2	10	12	2	10	12	7	32	39
Other commands/ installations	MEAN	6.7	5.8	5.9	6.5	6.3	6.4	5.7	6.9	6.6	6.2	6.3	6.3
	N	3	14	17	2	15	17	4	12	16	9	41	50
Central adjudication facility	MEAN	6.0	7.3	7.1	8.7	8.3	8.4	5.7	8.8	8.1	6.8	8.1	7.8
	N	3	15	18	3	15	18	3	11	14	9	41	50

Priority Placed by Different Groups on Continuing Assessment
(1="Very low priority" and 10="Very high priority")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Coworkers	MEAN	4.0	2.8	3.0	2.5	3.0	2.9	3.2	2.5	2.7	3.3	2.8	2.9
	N	3	14	17	2	15	17	4	13	17	9	42	51
Supervisors	MEAN	4.7	5.1	5.0	4.7	5.0	4.9	4.2	4.6	4.5	4.5	4.9	4.8
	N	3	14	17	3	15	18	4	13	17	10	42	52
First sergeant /Leading PO /Chief	MEAN	2.0	6.4	5.7	6.7	6.3	6.3	5.5	5.0	5.1	5.1	5.9	5.8
	N	2	11	13	3	15	18	4	10	14	9	36	45
Unit commanders	MEAN	5.0	6.8	6.5	8.0	6.5	6.8	7.0	4.6	5.2	6.7	6.1	6.2
	N	3	12	15	3	15	18	3	9	12	9	36	45
Installation commander	MEAN	5.3	6.1	5.9	3.5	6.7	6.9	8.0	5.7	6.2	7.2	6.2	6.3
	N	3	14	17	2	13	15	4	13	17	9	40	49
Unit security managers	MEAN	7.0	6.2	6.4	7.5	7.2	7.2	9.5	5.0	6.1	8.0	6.5	6.7
	N	2	12	14	2	15	17	2	6	8	6	33	39
Investigations office	MEAN	5.7	6.2	6.1	9.0	7.7	7.9	7.0	7.3	7.2	7.0	7.1	7.1
	N	3	13	16	2	15	17	3	13	16	8	41	49
Federal agencies	MEAN	5.0	5.9	5.7	7.0	5.8	6.0	6.5	6.1	6.1	6.0	5.9	6.0
	N	3	12	15	2	12	14	2	12	14	7	36	43
Personnel department	MEAN	3.0	4.1	3.9	5.0	3.9	4.0	2.5	3.0	2.9	3.2	3.7	3.6
	N	3	14	17	2	15	17	4	13	17	9	42	51
Medical department	MEAN	5.7	4.3	4.6	3.5	3.8	3.8	3.0	3.6	3.5	4.0	3.9	3.9
	N	3	13	16	2	15	17	4	13	17	9	41	50
Employee assistance groups	MEAN	2.0	2.6	2.6	2.5	4.0	3.8	4.7	3.6	3.9	3.5	3.4	3.4
	N	2	14	16	2	15	17	4	13	17	8	42	50
Legal office	MEAN	1.5	4.5	4.1	5.5	6.0	5.9	2.7	4.3	3.9	3.1	5.0	4.7
	N	2	13	15	2	15	17	4	13	17	8	41	49
Other security offices	MEAN	5.5	8.0	7.6	8.5	7.6	7.7	6.5	5.7	5.9	6.8	7.3	7.2
	N	2	10	12	2	13	15	2	7	9	6	30	36
Military/ Security Police	MEAN	4.0	6.8	[illegible]	9.0	8.3	8.4	2.7	5.8	5.0	5.1	7.1	6.7
	N	2	11	[illegible]	3	15	18	4	11	15	9	37	46
Other commands	MEAN	6.0	5.2	5.4	7.0	6.2	6.3	6.0	4.7	4.9	6.3	5.5	5.6
	N	3	13	16	2	14	16	2	10	12	7	37	44

(CONTINUED)

Priority Placed by Different Groups on Continuing Assessment
(1="Very low priority" and 10="Very high priority")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Senior intelligence personnel	MEAN	4.7	7.2	6.6	8.0	7.2	7.3	6.7	7.8	7.5	6.3	7.4	7.2
	N	3	9	12	2	12	14	4	10	14	9	31	40
Non-superv. personnel with access	MEAN	4.0	4.4	4.3	4.0	4.0	4.0	3.7	3.2	3.3	3.9	3.9	3.9
	N	3	14	17	2	14	16	4	13	17	9	41	50
Non-superv. personnel without access	MEAN	1.5	3.1	2.9	3.0	3.5	3.5	.	1.9	1.9	2.0	2.9	2.8
	N	2	14	16	1	14	15	0	12	12	3	40	[illegible]

How well do groups understand their CA responsibilities?
(1="Not well at all" and 10="Extremely well")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Supervisors	MEAN	7.0	5.9	6.1	6.3	5.1	5.3	6.7	4.5	5.0	6.7	5.2	5.5
	N	3	15	18	3	15	18	4	13	17	10	43	53
Cleared Individuals	MEAN	6.7	4.9	5.2	5.7	5.6	5.6	5.7	4.4	4.7	6.0	5.0	5.2
	N	3	15	18	3	15	18	4	13	17	10	43	53
Uncleared Individuals	MEAN	1.5	3.4	3.2	6.5	3.5	3.9	6.0	2.5	3.0	4.7	3.2	3.4
	N	2	14	16	2	14	16	2	11	13	6	39	45

Types of Information Maintained in Separate Files
(Number of Respondents Indicating Each Type)

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Disciplinary actions, NJPs	3	9	12	1	3	4	4	7	11	8	19	27
Local violations	2	12	14	1	10	11	4	5	9	7	27	34
Sec.-related performance appraisal info	1	1	2	0	2	2	2	3	5	3	6	9
Security violations and incidents	2	9	11	2	12	14	4	7	11	8	28	36
Personal history information	3	10	13	1	8	9	4	3	7	8	21	29
Personal information	3	8	11	2	1	3	3	6	9	8	15	23
Unfavorable Information Files	2	10	12	0	4	4	4	4	8	6	18	24
Special Security Files	3	0	3	1	14	15	3	1	4	7	15	22
Other	1	4	5	2	1	3	0	1	1	3	6	9

Are any periodic reports to continuing assessment
prepared by the security office?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	.	5	5	2	5	7	.	13	13	2	23	25
Yes	3	10	13	1	10	11	2	1	3	6	21	27

Percentage of each group evaluated on security
as part of their regular performance evaluation

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Unit Commanders	MEAN	0.0	4.6	3.7	100.0	0.2	21.6	0.0	22.2	16.7	33.3	7.9	13.4
	N	3	13	16	3	11	14	3	9	12	9	33	42
Supervisors	MEAN	0.0	8.9	7.4	100.0	10.5	29.6	0.0	15.0	11.0	30.0	11.3	15.3
	N	3	14	17	3	11	14	4	11	15	10	36	46
Cleared Non-supervisory Personnel	MEAN	0.0	12.5	10.3	100.0	4.5	25.0	0.0	2.7	2.0	30.0	7.1	12.1
	N	3	14	17	3	11	14	4	11	15	10	36	46

Percentage of each group evaluated specifically on continuing assessment
as part of their regular performance evaluation

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Unit Commanders	MEAN	0.0	4.6	3.7	33.3	0.0	7.7	0.0	0.0	0.0	10.0	1.8	3.6
	N	3	13	16	3	10	13	4	11	15	10	34	44
Supervisors	MEAN	0.0	6.4	5.3	33.3	0.2	8.5	0.0	0.0	0.0	10.0	2.6	4.3
	N	3	14	17	3	9	12	4	12	16	10	35	45

Percentage of inspection time devoted to continuing assessment

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	11.7	23.0	21.1	37.0	28.3	29.8	15.3	7.3	9.2	20.7	20.1	20.2
	N	3	15	18	3	15	18	4	13	17	10	43	53

Components of the Security Education Program
(Number of Programs Providing the Component)

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Info on individual's CA responsibilities	2	11	13	3	13	16	4	8	12	9	32	41
Guidance on pers. security indicators	1	9	10	3	10	13	3	10	13	7	29	36
Reference info on identifying risks	1	6	7	0	9	9	2	6	8	3	21	24
Guidance on reporting derogatory info	2	12	14	1	11	12	4	10	14	7	33	40
Info on obtaining assistance, counseling	2	7	9	2	6	8	3	5	8	7	18	25

Percentage of cleared personnel requiring access to classified information
on a day-to-day basis who participated in
personnel security education in the past 12 months

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	83.3	80.9	81.3	52.3	60.0	58.6	91.2	61.2	68.7	77.2	68.5	70.2
	N	3	16	19	3	13	16	4	12	16	10	41	51

Percentage of non-cleared personnel who received
security eduucation training in the past 12 months

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	62.5	66.5	66.0	21.0	42.7	39.6	.	48.0	48.0	41.7	53.4	52.3
	N	2	14	16	2	12	14	0	10	10	4	36	40

Do initial briefings contain any information on
reporting responsibilities in continuing assessment?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	.	1	1	.	1	1	1	3	4	1	5	6
Yes	3	13	16	3	12	15	2	10	12	8	35	43

Percentage of initial briefings devoted to continuing assessment

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	23.3	25.9	25.4	7.3	43.6	35.9	65.0	28.3	34.4	27.8	32.5	31.6
	N	3	12	15	3	11	14	2	10	12	8	33	41

Percentage of cleared personnel with access to classified information who have had a refresher briefing in the past year

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	65.0	80.5	77.9	44.0	61.9	58.3	88.3	46.7	55.0	65.8	64.4	64.6
	N	3	15	18	3	12	15	3	12	15	9	39	48

Do refresher briefings cover continuing assessment responsibilities?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	.	3	3	.	2	2	.	6	6	.	11	11
Yes	3	11	14	3	10	13	3	5	8	9	26	35

Percentage of refresher briefings devoted to continuing assessment

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage	MEAN	16.7	22.0	20.9	39.0	47.5	45.5	45.0	40.0	41.9	33.6	35.3	34.8
	N	3	11	14	3	10	13	3	5	8	9	26	35

What continuing assessment topics are covered?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Security risk indicators												
No	1	7	8	3	5	8	2	9	11	6	21	27
Yes	2	9	11	2	10	12	2	5	7	6	24	30
Reporting mechanisms												
No	.	7	7	3	5	8	2	10	12	5	22	27
Yes	3	9	12	2	10	12	2	4	6	7	23	30
Security threats												
No	.	6	6	2	5	7	1	9	10	3	20	23
Yes	3	10	13	3	10	13	3	5	8	9	25	34
Other												
No	1	11	12	5	12	17	4	14	18	10	37	47
Yes	2	5	7	.	3	3	.	.	.	2	8	10

Is security counseling available for individuals
who have personal problems that might have bearing
on their eligibility for a security clearance or access?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	.	5	5	.	6	6	.	2	2	.	13	13
Yes	3	10	13	3	9	12	4	11	15	10	30	40

Do individuals who conduct counseling on security-related matters
typically have an extensive background and knowledge
of the vulnerabilities for the type of security-related matter involved?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	2	8	10	.	8	8	1	5	6	3	21	24
Yes	1	7	8	3	5	8	3	8	11	7	20	27

Are supervisors generally awar~ of when and how
to refer individuals for security counseling?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	2	5	7	.	10	10	.	7	7	2	22	24
Yes	1	8	9	3	4	7	4	6	10	8	18	26

Rate the quality of security training in continuing assessment
(1="Very poor" and 10="Excellent")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Training for security office staff	MEAN	2.3	4.1	3.8	5.0	6.1	5.9	1.3	3.3	2.7	2.7	4.6	4.2
	N	3	15	18	3	14	17	4	11	15	10	40	50
Training for unit security managers	MEAN	1.0	3.9	3.5	5.3	6.1	6.0	2.5	1.2	1.6	3.3	4.5	4.3
	N	2	13	15	3	14	17	2	5	7	7	32	39

Extent there is sufficient information
to adequately meet CA responsibilities
(1="Very little information" and 10="Complete information")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
For unit commanders	MEAN	5.7	6.5	6.3	7.3	7.1	7.1	6.0	5.2	5.5	6.3	6.4	6.4
	N	3	13	16	3	15	18	3	8	11	9	36	45
For the security office	MEAN	5.3	5.3	5.3	5.0	6.6	6.3	7.2	5.2	5.6	6.0	5.7	5.8
	N	3	13	16	3	15	18	4	13	17	10	41	51

How much additional valid derogatory information would be generated
if most derogatory information was forwarded to
both the security office and unit commander at the same time?

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Percentage added	MEAN	43.3	43.5	43.4	50.0	65.7	63.8	33.7	28.8	30.0	40.6	47.0	45.8
	N	3	13	16	2	15	17	4	13	17	9	41	50

In general, how much emphasis in the continuing assessment program is given to personnel who do not have security clearances (as opposed to the emphasis given to those with clearances)?

	Army			Air Force			Navy		Total		
	SCI	Col.	Total	SCI	Col.	Total	Col.	Total	SCI	Col.	Total
No emphasis	1	5	6	1	1	2	4	4	2	10	12
Much less emphasis	1	3	4	1	1	2	2	2	2	6	8
Less Emphasis	.	2	2	.	4	4	1	1	.	7	7
Somewhat less	.	1	1	.	1	1	.	.	.	2	2
About the same	.	4	4	.	5	5	3	3	.	12	12

Given current resources, do you think personnel without security clearances should be included in the continuing assessment program?

	Army			Air Force		Navy			Total		
	SCI	Col.	Total	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	1	5	6	3	3	.	1	1	1	9	10
Yes	1	10	11	10	10	1	11	12	2	31	33

In general, how much emphasis in the continuing assessment program is given to personnel who have clearance eligibility as opposed to those with clearances and access to classified information?

	Army			Air Force		Navy		Total		
	SCI	Col.	Total	Col.	Total	Col.	Total	SCI	Col.	Total
No emphasis	1	1	2	.	.	.	.	1	1	2
Much less emphasis	.	1	1	.	.	3	3	.	4	4
Less Emphasis	.	1	1	5	5	2	2	.	8	8
Somewhat less	.	3	3	3	3	1	1	.	7	7
About the same	1	10	11	7	7	6	6	1	23	24

Is more continuing assessment effort directed to
persons with Top Secret clearances
as opposed to persons with Secret clearances at this installation?

	Army			Air Force		Navy			Total		
	SCI	Col.	Total	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No		9	9	9	9	1	10	11	1	28	29
Yes	2	7	9	6	6	.	4	4	2	17	19

Is more continuing assessment effort directed to particular positions
at this installation?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
No	1	10	11	1	7	8	3	7	10	5	24	29
Yes	2	6	8	1	7	8	1	7	8	4	20	24

Current Effectiveness of CA Program Components
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
DoD security regulations	MEAN	4.7	6.1	5.8	5.3	3.9	4.2	6.5	4.2	4.9	5.6	4.8	5.0
	N	3	15	18	3	14	17	4	10	14	10	39	49
Service branch CA regulations	MEAN	5.0	5.1	5.1	5.7	5.7	5.7	6.7	6.1	6.2	5.9	5.6	5.7
	N	3	15	18	3	14	17	4	13	17	10	42	52
Local CA regulations	MEAN	6.0	4.9	5.1	5.0	5.4	5.3	3.5	3.7	3.6	4.7	4.7	4.7
	N	3	15	18	3	13	16	4	13	17	10	41	51
Indicators of security risk	MEAN	4.7	6.1	5.9	5.0	4.8	4.8	5.7	5.2	5.4	5.2	5.4	5.4
	N	3	14	17	3	14	17	4	13	17	10	41	51
Sources of derogatory information	MEAN	4.7	5.9	5.7	5.3	5.9	5.8	6.2	5.7	5.8	5.5	5.8	5.7
	N	3	15	18	3	14	17	4	13	17	10	42	52
CA reporting procedures	MEAN	4.3	4.9	4.8	7.0	5.2	5.5	5.5	4.8	5.0	5.6	5.0	5.1
	N	3	15	18	3	14	17	4	13	17	10	42	52
Coordination of information	MEAN	1.3	4.4	3.9	4.0	4.4	4.4	5.0	3.0	3.5	3.6	4.0	3.9
	N	3	15	18	3	14	17	4	13	17	10	42	52
CA recordkeeping procedures	MEAN	6.3	4.7	4.9	8.0	5.1	5.6	4.7	4.0	4.2	6.2	4.6	4.9
	N	3	15	18	3	14	17	4	13	17	10	42	52
Performance appraisal information	MEAN	0.0	0.6	0.5	5.0	2.3	2.8	1.0	1.5	1.4	1.9	1.4	1.5
	N	3	15	18	3	14	17	4	13	17	10	42	52
Incentives for reporting	MEAN	0.0	0.6	0.5	1.7	1.4	1.4	1.3	0.5	0.6	1.0	0.8	0.8
	N	3	15	18	3	14	17	4	13	17	10	42	52
Inspections/ staff assistance visits	MEAN	2.3	4.1	3.8	7.7	3.9	4.6	4.0	1.8	2.4	4.6	3.4	3.6
	N	3	15	18	3	14	17	4	13	17	10	42	52
Indicators of CA program effectiveness	MEAN	4.0	4.9	4.7	6.3	3.9	4.3	2.2	1.9	2.0	4.0	3.6	3.7
	N	3	15	18	3	14	17	4	13	17	10	42	52
Employee assistance programs	MEAN	2.7	2.5	2.5	5.0	3.9	4.1	6.5	3.8	4.4	4.9	3.3	3.6
	N	3	15	18	3	14	17	4	13	17	10	42	52
Security counseling	MEAN	4.7	3.5	3.7	6.0	3.4	3.8	6.0	3.9	4.4	5.6	3.6	4.0
	N	3	14	17	3	14	17	4	13	17	10	41	51
Security education	MEAN	5.7	5.5	5.5	5.3	5.1	5.2	5.7	4.4	4.7	5.6	5.0	5.1
	N	3	15	18	3	14	17	4	13	17	10	42	52

(CONTINUED)

Current Effectiveness of CA Program Components
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Security office training in CA	MEAN	1.7	3.4	3.1	7.3	4.6	5.1	3.0	3.1	3.1	3.9	3.7	3.7
	N	3	15	18	3	14	17	4	13	17	10	42	52
Unit security staff training in CA	MEAN	1.3	4.4	3.9	6.3	4.9	5.2	3.3	1.1	1.8	3.7	4.0	3.9
	N	3	14	17	3	14	17	3	7	10	9	35	44
Security briefings	MEAN	5.7	5.3	5.3	7.0	4.6	5.0	6.2	4.9	5.2	6.3	4.9	5.2
	N	3	15	18	3	14	17	4	13	17	10	42	52
Clearance susp./revocation process	MEAN	3.7	6.2	5.8	7.0	7.2	7.2	7.0	6.6	6.7	6.0	6.7	6.5
	N	3	15	18	3	14	17	4	12	16	10	41	51
Overall CA for military personnel	MEAN	5.3	5.3	5.3	7.7	5.4	5.8	6.0	4.9	5.2	6.3	5.2	5.4
	N	3	15	18	3	14	17	4	12	16	10	41	51
Overall CA for civilian personnel	MEAN	4.7	4.0	4.1	5.0	4.0	4.2	4.7	3.7	4.0	4.8	3.9	4.1
	N	3	15	18	3	14	17	3	8	11	9	37	46

Potential Effectiveness of CA Program Components
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
DoD security regulations	MEAN	8.3	9.1	8.9	8.0	4.9	5.5	7.7	7.2	7.4	8.0	7.1	7.2
	N	3	14	17	3	14	17	4	10	14	10	38	48
Service branch CA regulations	MEAN	8.3	9.4	9.2	8.7	7.6	7.8	8.5	8.4	8.4	8.5	8.4	8.5
	N	3	14	17	3	14	17	4	13	17	10	41	51
Local CA regulations	MEAN	8.7	7.3	7.5	8.7	7.5	7.7	5.5	8.4	7.7	7.4	7.7	7.6
	N	3	14	17	3	14	17	4	12	16	10	40	50
Indicators of security risk	MEAN	8.3	8.5	8.5	7.7	7.9	7.8	7.0	8.0	7.8	7.6	8.1	8.0
	N	3	14	17	3	14	17	4	13	17	10	41	51
Sources of derogatory information	MEAN	9.0	9.0	9.0	8.7	9.1	9.0	8.3	8.2	8.2	8.6	8.8	8.7
	N	3	14	17	3	14	17	4	13	17	10	41	51
CA reporting procedures	MEAN	8.3	8.8	8.7	9.0	8.1	8.3	8.5	7.8	8.0	8.6	8.3	8.3
	N	3	14	17	3	14	17	4	13	17	10	41	51
Coordination of information	MEAN	8.5	9.1	9.1	8.3	7.5	7.7	6.0	7.0	6.8	7.3	7.9	7.8
	N	2	14	16	3	15	18	4	13	17	9	42	51
CA recordkeeping procedures	MEAN	7.7	8.6	8.5	9.0	7.9	8.1	6.7	6.8	6.8	7.7	7.8	7.8
	N	3	14	17	3	14	17	4	13	17	10	41	51
Performance appraisal information	MEAN	6.3	7.1	7.0	7.0	5.9	6.1	4.0	5.6	5.2	5.6	6.2	6.1
	N	3	14	17	3	14	17	4	13	17	10	41	51
Incentives for reporting	MEAN	2.7	6.2	5.6	5.0	6.9	6.6	5.0	4.8	4.9	4.3	6.0	5.7
	N	3	14	17	3	15	18	4	12	16	10	41	51
Inspections/ staff assistance visits	MEAN	8.0	7.6	7.6	8.7	8.2	8.3	8.8	6.8	7.3	8.6	7.6	7.8
	N	2	14	16	3	15	18	4	12	16	9	41	50
Indicators of CA program effectiveness	MEAN	7.3	8.4	8.2	7.7	6.6	6.8	6.2	6.6	6.5	7.0	7.2	7.2
	N	3	14	17	3	14	17	4	12	16	10	40	50
Employee assistance programs	MEAN	7.3	8.3	8.1	8.3	7.7	7.8	7.2	7.6	7.5	7.6	7.9	7.8
	N	3	14	17	3	14	17	4	13	17	10	41	51
Security counseling	MEAN	6.7	7.6	7.5	8.3	7.6	7.7	7.7	7.9	7.9	7.6	7.7	7.7
	N	3	14	17	3	14	17	4	13	17	10	41	51
Security education	MEAN	8.7	9.1	8.2	8.7	9.0	8.9	9.0	8.1	8.3	8.8	8.4	8.5
	N	3	14	17	3	14	17	4	13	17	10	41	51

(CONTINUED)

Potential Effectiveness of CA Program Components
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Security office training in CA	MEAN	8.0	8.3	8.2	9.0	8.9	8.9	8.8	7.7	8.0	8.6	8.3	8.4
	N	3	14	17	3	14	17	4	12	16	10	40	50
Unit security staff training in CA	MEAN	8.0	7.5	7.5	8.7	8.4	8.4	9.5	7.0	7.6	8.7	7.8	7.9
	N	2	13	15	3	14	17	2	6	8	7	33	40
Security briefings	MEAN	8.3	7.9	7.9	8.7	8.0	8.1	8.5	7.8	8.0	8.5	7.9	8.0
	N	3	14	17	3	14	17	4	12	16	10	40	50
Clearance susp./revocation process	MEAN	7.7	8.5	8.4	8.7	9.1	9.1	8.5	7.7	7.9	8.3	8.5	8.4
	N	3	14	17	3	14	17	4	13	17	10	41	51
Overall CA for military personnel	MEAN	8.7	8.6	8.6	9.0	8.5	8.6	9.0	8.3	8.4	8.9	8.4	8.5
	N	3	14	17	3	13	16	4	12	16	10	39	49
Overall CA for civilian personnel	MEAN	8.3	6.9	7.1	9.0	8.1	8.3	7.7	8.1	8.0	8.3	7.6	7.7
	N	3	14	17	3	13	16	3	8	11	9	35	44

How would you rate the effectiveness of
periodic reinvestigations at your installation?
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Overall Effectiveness	MEAN	6.3	6.9	6.8	8.3	7.4	7.6	7.3	6.2	6.4	7.3	6.9	7.0
	N	3	15	18	3	14	17	3	13	16	9	42	51

How would you rate the overall effectiveness of
the current continuing assessment program at your installation?
(1="Very ineffective" and 10="Very effective")

		Army			Air Force			Navy			Total		
		SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Overall Effectiveness	MEAN	5.7	5.5	5.6	6.3	6.2	6.2	7.2	5.0	5.5	6.5	5.6	5.8
	N	3	15	18	3	15	18	4	13	17	10	43	53

Overall, which type of continuing assessment program is better,
one which reports only significant derogatory information to adjudication
and suspends an individual's access pending final adjudication or
one which reports all derogatory information to adjudication and
may or may not suspend an individual's access?

	Army			Air Force			Navy			Total		
	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total	SCI	Col.	Total
Signif. Derog.	.	5	5	.	8	8	2	4	6	2	17	19
All Derog. Info	3	10	13	3	7	10	2	8	10	8	25	33